Proposed Redacted Version of Exhibit 4 to the Deckant Declaration (Dkt. No. 259-7)

EXHIBIT 4

UNREDACTED

THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE META PIXEL TAX FILING CASES

This document relates to:

All Actions

Master File No. 5:22-cv-07557-PCP (VKD)

REPLY REPORT OF ROBERT ZEIDMAN

REPLY REPORT OF ROBERT ZEIDMAN

Contents

I, Robert Zeidman, provide the following expert disclosures.

I. INTRODUCTION

1. Based on my background and experience, I have been asked by counsel for the Plaintiffs in this action to provide a reply to the Corrected Rebuttal Expert Report of Georgios Zervas, Ph.D. ("Zervas Report") and to points raised by Defendant Meta Platforms, Inc. ("Meta") in its Motion to Exclude the Expert Report and Testimony of Robert Zeidman ("the Motion" or "Mot."), Dkt. 233.

2. For my work on this matter Zeidman Consulting is being compensated at a rate of $1,000.00 per hour.

3. In reaching the opinions and conclusions discussed herein, I relied upon the following materials:

a. Corrected Rebuttal Expert Report of Georgios Zervas, Ph.D. ("Zervas Report")
b. Motion to Exclude the Expert Report and Testimony of Robert Zeidman ("the Motion" or "Mot.")
c. Expert Report of Robert Zeidman ("Zeidman Report")
d. Transcript of Deposition of Robert Zeidman ("Zeidman Dep.")
e. California Penal Code § 638.50
f. Rebuttal Expert Report of Steven Tadelis ("Tadelis Report")
g. Exhibit A: GeeksforGeeks, TCP/IP Model, https://www.geeksforgeeks.org/computer-networks/tcp-ip-model
h. Exhibit B: Maxmind, "Geolocation accuracy" https://support.maxmind.com/knowledge-base/articles/maxmind-geolocation-accuracy
i. Exhibit C: James Sanders, "IP Geolocation in 2025: A Comprehensive Guide to Location Intelligence," litport, https://litport.net/blog/ip-

geolocation-a-comprehensive-guide-to-location-intelligence-69228

j. Exhibits D: ad_pixels_traffic table

k. Exhibit E: offsite_signals table

l. Exhibit F: offsite_signals_pipe table

m. Exhibit G: PIXEL_TAX000058898-905

n. Exhibit H: Thales Cybersecurity, HTTP/2, https://www.imperva.com/learn/performance/http2

o. Exhibit I: Adams, Scarlett, What is a Session ID? Everything You Need to Know, the knowledge academy, November 4, 2025

p. Exhibit J: IONOS Digital Guide, What is a session ID?, April 4, 2021, https://www.ionos.com/digitalguide/hosting/technical-matters/what-is-a-session-id

q. Exhibit K: SecureCoding, Session Management: An Overview, April 29, 2021, https://www.securecoding.com/blog/session-management-an-overview

r. Exhibit L: SQL Code-Discarded Entries

s. Exhibit M: Transcript of Deposition of Abhinav Anand in Meta Healthcare

t. Exhibit N: Errata Sheet for Transcript of Deposition of Abhinav Anand in Meta Healthcare

u. Exhibit O: 30(b)(6) Deposition of Tobias Wooldridge in Meta Healthcare

v. Exhibit P: SQL Code-Visits

w. Exhibit Q: SQL Code-Tax Information & Populated by Number

II. TECHNICAL BACKGROUND

4. In this section I provide additional technical background helpful for understanding aspects of my reply report.

A. TCP/IP Model for Internet Communications[1]

5. The TCP/IP model serves as a framework for understanding communication within a network, as shown in Figure 1.

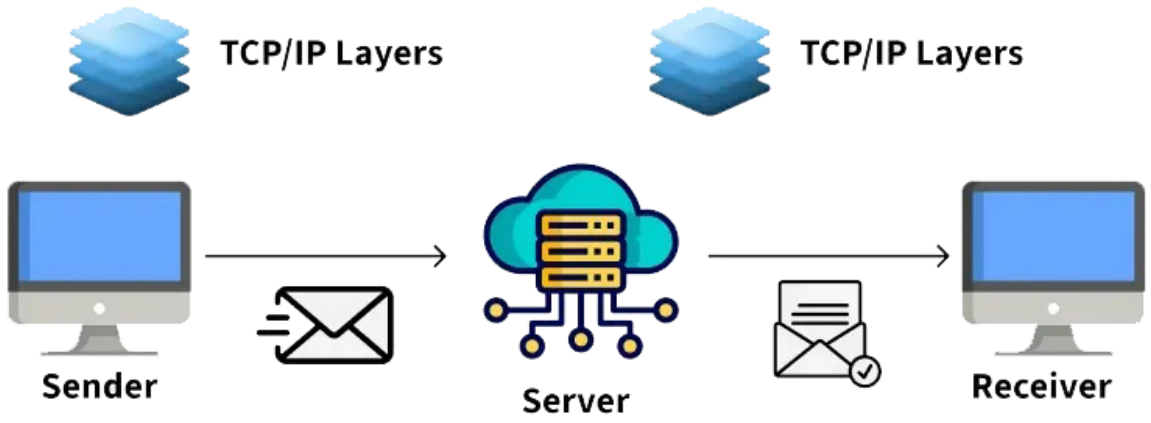


Figure 1. TCP/IP Model Example

6. It organizes various networking protocols into five layers: Application, Transport, Network (e.g., Internet), Data Link, and Physical. While the OSI model consists of seven layers, today's networks generally use the simpler 5-layer TCP/IP model as shown in Figure 2.

[1] *See* GeeksforGeeks, *TCP/IP Model*, https://www.geeksforgeeks.org/computer-networks/tcp-ip-model, attached as **Exhibit A**.

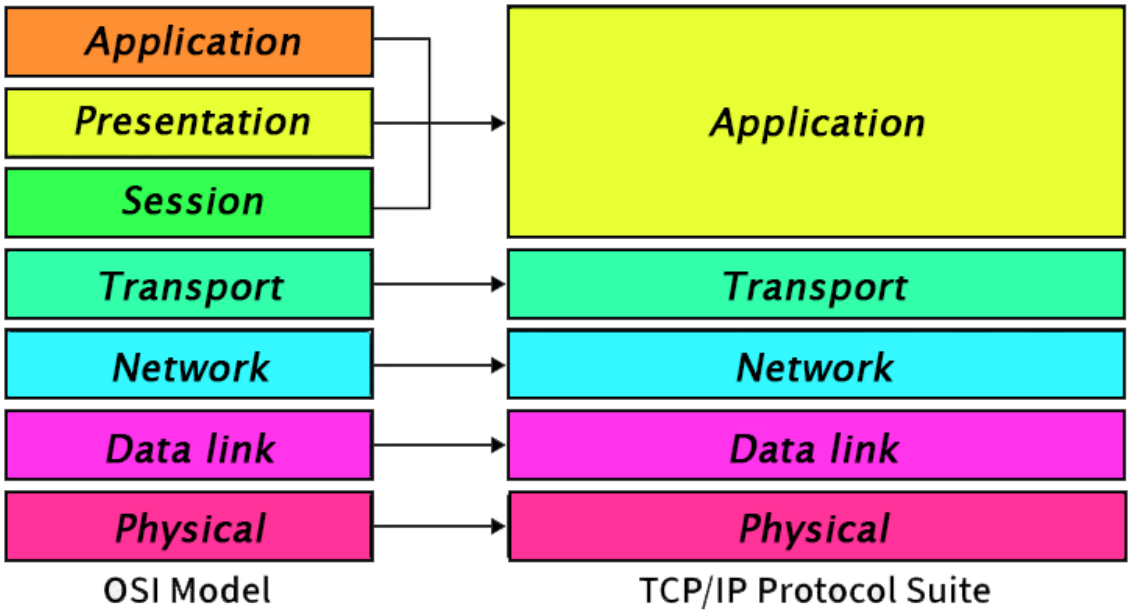


Figure 2. OSI Model vs. TCP/IP Model

7. A core objective of TCP/IP is to ensure data sent by one party reaches the recipient both safely and accurately. To achieve this, information is divided into packets before transmission. Each packet may travel a different path through the network, but they are all reassembled in order upon arrival at their destination.

8. The Network layer of the TCP/IP model uses the Internet Protocol (IP) to assign a unique IP address to every device connected to the network. Each packet contains a source IP address indicating where the packet is coming from and a destination IP address indicating where each packet is going.

9. The location of a device can be identified with an IP address. Generally, IP geolocation tracking at the country and state level is highly reliable. Companies that specialize in geolocation report that the technology can identify the state of an IP address with 80% to 95%

accuracy, though a VPN can obscure that information.[2,3]

III. BACKGROUND FACTS

10. In Meta's Motion to exclude my report and testimony, my background and experience are misconstrued by Meta. Everything referred to in this section can be found on my resume submitted as Exhibit B to my initial expert report. *See* Expert Report of Robert Zeidman ("Zeidman Report", ECF No. 214-1), Ex. B.

11. Meta claims that I am "an electrical engineer who concentrated his expert career in intellectual property matters—not data privacy—to opine on the Meta Pixel in support of [Plaintiff's] Class Cert Motion." Mot. at 4. This implies that electrical engineering is my only skill, but that is not true. I have two degrees in electrical engineering but also one in physics. *See* Zeidman Report ¶ 6. I have developed software for about 50 years, beginning in middle school up until today. *See* Zeidman Report ¶ 6. I personally wrote the code and commercialized the CodeSuite® program, the CodeMeasure® program, the SynthOS® program, the Molasses® program, and the client software and server software for eVAULT Remote Backup Service. *See* Zeidman Report ¶¶ 7-8, Ex. B. I have supervised the development of several enterprise software systems including at my companies Firtiva Corporation, Software Analysis and Forensic Engineering Corporation, and Good Beat Games, Inc. *See* Zeidman Report ¶¶ 7-8, Ex. B. I have written papers, articles, and a textbook on software forensics. *See* Zeidman Report ¶ 9, Ex. B. I have won awards for software forensics including three from the international Institute of Electrical and Electronics Engineers ("IEEE") of which I am a Life Member. *See* Zeidman Report, Ex. B. Even as far back as when I was a high school student, I was given an award from the national

[2] Maxmind, "Geolocation accuracy" https://support.maxmind.com/knowledge-base/articles/maxmind-geolocation-accuracy, retrieved December 12, 2025, attached at **Exhibit B**.

[3] James Sanders, "IP Geolocation in 2025: A Comprehensive Guide to Location Intelligence," litport, https://litport.net/blog/ip-geolocation-a-comprehensive-guide-to-location-intelligence-69228, May 23, 2025, attached as **Exhibit C**.

Association for Educational Data Systems for the coding of a source code interpreter. *See* Zeidman Report, Ex. B. With specific regard to data privacy, I wrote the article "How much does your thermostat know about you?" that was published in *IT World* magazine on July 30, 2015. *See* Zeidman Report, Ex. B.

12. Meta further asserts that I have "never been qualified as an expert in data privacy, nor [have I] given expert testimony at a deposition or at a hearing on data privacy." Mot. at 4. As I stated at my deposition, apart from this case I have not [yet] given testimony on data privacy at a deposition or at a hearing, but it is incorrect that I have never been qualified as an expert in data privacy. *See* Tr. of Oct. 3, 2025 Dep. of Robert Zeidman ("Zeidman Dep.") at 19:11-20:8. As my resume shows, *see* Zeidman Report, Ex. B, I was the expert for the plaintiffs in *In Re: TikTok, Inc., Consumer Privacy Litigation*, 1:20-cv-04699 (N.D. Ill.), where I was retained by the plaintiffs as a source code expert to assess TikTok's technical functions, *see* Zeidman Report, Ex. B, ECF No. 316 at 7. As I further stated in my deposition, I have also been an expert in other privacy suits where I was not publicly disclosed and thus have an obligation to keep those cases confidential. *See* Zeidman Dep. at 19:11-20:23.

13. Meta further asserts, "There is nothing in his published works that involves anything related to pixel technologies, their data transmissions, or even consumer data more generally." Mot. at 4. This is also incorrect. As I stated in my deposition, I started the company Firtiva with the purpose of providing streaming media that tracked user preferences and used those preferences to target advertising. *See* Zeidman Dep. at 15:22-16:23. At the time that I developed the technology, it was not called "pixels" and there was no Meta. *See* Zeidman Dep. at 15:22-16:23. I not only supervised the development of the streaming platform and the tracking mechanism, but I also filed and was awarded two patents on the technology: U.S. 8,316,390, filed in 2001 and issued in 2012, and U.S. 10,116,999, filed in 2012 and issued in 2018. *See* Zeidman Dep. at 15:22-16:23; Zeidman Report, Ex. B. Both patents were entitled "Method for advertisers to sponsor broadcasts without commercials." *See* Zeidman Report, Ex. B.

14. I also developed the software and the system of my earlier company, eVAULT

Remote Backup Service, where I needed to understand privacy issues with regard to data being backed up by customers to the company's server. *See* Zeidman Report, ¶ 8, Ex. B. I wrote an article about this system for the April/May/June 1996 issue of *Disaster Recovery Journal* entitled "An Introduction to Remote Backup." *See* Zeidman Report, Ex. B. I also wrote a paper that I presented at IEEE Jamcon 1995 entitled "Remote Backup - Transmitting Critical Data Over Phone Lines for Offsite Storage." *See* Zeidman Report, Ex, Ex. B.

IV. REPLY

15. In this section I respond to the criticisms raised in the Zervas Report and Meta's Motion.

A. Definitions

16. In Meta's Motion, my understanding of following terms was misconstrued. To be clearer, I provide my understanding of the following terms in the next sections of this report: (1) "pen register" data; (2) tax information; and (3) uniform.

i. *Pen register data*

17. In my report, I referred to California Penal Code § 638.50 defining a "pen register" as a "device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication." *See* Zeidman Report ¶ 4 & n.2. I did not intend to, and did not, offer my understanding of the legal meaning of this statute. Instead, I used the term "pen register" data as a shorthand to refer to "dialing, routing, addressing, or signaling information" as I understood it, and how it related to data transmitted by the Meta Pixel. *See* Zeidman Report ¶¶ 28-29, 57. I did not intend to, and did not, make a determination whether Meta violated California Penal Code § 638.50, which is not within my area of expertise or my authority to decide. I only meant to show that from a technological perspective, the Meta

Pixel sends the type of data that I understand to be "pen register" data (i.e., dialing, routing, addressing, or signaling information). *See* Zeidman Report ¶¶ 28-29, 57.

18. The Hive data produced by Meta includes tables with fields clearly marked as "city," "country," "geo_ip_zip," and IP addresses. Based on Meta's internal documents, the `ad_pixels_traffic`, `offsite_signals`, and `offsite_signals_pipe` tables[4] in the Meta Hive all include the fields city, country, and geo_ip_zip, and an IP address field of some kind.

19. As I discussed in my initial report at ¶ 29, Meta produced a data dictionary that provides that the fields "city" and "country" represent the city and country "where the pixel is fired (inferred from geo IP location)." PIXEL_TAX000058899.[5] There is also the field "geo_ip_zip," which the data dictionary describes as "[t]he zip code where the pixel is fired." PIXEL_TAX000058900.[6] I understand this data to be addressing information because it provides a physical location where the information originates from. The fact that this information is in Meta's Hive data means that Meta is able to use the information sent to it to identify the city and state of origin of the information.

20. Further, all Internet communication is based on the TCP/IP model using the Hypertext Transfer Protocol ("HTTP")[7] as the Application Layer. Data from the user is sent using HTTP packets via the Meta Pixel to Meta. These packets are built upon packets at the lower-level IP layer. Such packets include the source IP address and destination IP address in its header, which I understand to be addressing information because these IP addresses provide Internet locations for the source and destination (the destination being Meta).

21. The data collected by the Meta Pixel includes the source URL in the field

[4] The tables are attached to this report as **Exhibits D (**ad_pixels_traffic table**); Exhibit E** (offsite_signals table) and **Exhibit F** (offsite_signals_pipe table).

[5] This document is attached to this report as **Exhibit G**.

[6] This document is attached to this report as **Exhibit G**.

[7] Thales Cybersecurity, HTTP/2, https://www.imperva.com/learn/performance/http2, retrieved December 3, 2025, attached as **Exhibit H**.

`resolved_document_link`, which Meta's data dictionary describes as "[t]he URL we think the pixel fired from." PIXEL_TAX000058899. The data collected by the Meta Pixel also includes the domain of the user's email address in the field `known_private_email_domain`, which Meta's data dictionary describes as "[t]he domain of the email address used as PII for this event." PIXEL_TAX000058901. I understand these data to be addressing information because these URLs represent the source of the information on the Internet.

22. Dr. Zervas does not dispute that this information is transmitted to Meta.[8,9]

23. As I discussed in my report, a Meta Developer's page at https://developers.facebook.com/docs/meta-pixel explains that the Meta Pixel can collect, among other things, "[a]nything that is generally present in HTTP headers, a standard web protocol sent between any browser request and any server on the internet. This information may include data like IP addresses, information about the web browser, page location, document, referrer and person using the website." *See* Zeidman Report ¶ 29, Ex. G. I understand this data to be routing, addressing, and signaling information.

ii. *Tax information*

24. I did not specifically define the term "tax information" because I believe there is a common sense definition that would refer to any information that would typically be found on a tax form, particularly financial information. Thus it would include things like revenue, number of dependents, W2 forms, adjusted gross income (AGI), federal taxes owed, and tax refund amount.

[8] "These data transmissions also include such information as IP addresses, standard HTTP data . . . ." Zervas Report ¶ 16.

[9] "'The Meta Pixel can collect the following data: Http Headers – Anything that is generally present in HTTP headers, a standard web protocol sent between any browser request and any server on the internet. This information may include data like IP addresses, information about the web browser, page location, document, referrer and person using the website.". Zervas report, footnote 41 (citing "Meta Pixel," *Meta*, https://developers.facebook.com/docs/meta-pixel/, accessed October 25, 2025).

Meta "admit[ted] that it received from the TaxAct website via the Pixel, among other things, parameters bearing the labels 'num_of_dependents,' 'w2,' 'agi,' 'federal_owe_amount,' and "federal_refund_amount." *See* Zeidman Report Ex. N. These fields are clearly descriptive of information that would comprise tax information.

iii. *Uniformity*

25. In my report, I state that "[d]uring the relevant class periods the Meta Pixel operated in a largely uniform manner on the Tax Preparers' websites with respect to the basic mechanics of collecting and transmitting visitor data to Meta." Zeidman Report ¶ 40. I repeat a similar statement in my conclusions in section VI. *See* Zeidman Report ¶ 57. To reiterate, I use the term "largely uniform" to mean that the Meta Pixel utilized the same mechanisms to collect and transmit data during the class periods, regardless of any changes in the specific data that the individual Tax Websites collected. These mechanisms consist of standard events, automatic events, and custom events. *See* Zeidman Report ¶¶ 31, 36. The automatic event data collected during the class periods did not change. Even if the standard event data and custom event data collected for each visit to the Tax Preparer websites may have varied, my review showed that the kinds of events the Meta Pixel collected and transmitted remained largely uniform during the class periods. To further clarify, my opinion is *not* that the Meta Pixel operated in a largely uniform manner across *both* the H&R Block and TaxAct websites, as compared to each other, but that each website's Meta Pixel individually operated in a largely uniform manner.

B. My Proposed Method for Counting Visits to the H&R Block and TaxAct Websites Are Not Flawed

26. Dr. Zervas claims that my methods for counting visits to the Tax Preparers' websites are flawed. *See* Zervas Report ¶¶ 46-61. I address each specific criticism and explain below why they are not flawed.

i. *My Proposed Method for Counting Visits to the H&R Block and TaxAct Websites Are Reliable*

a. By definition, each session ID equates to a unique website visit

27. Dr. Zervas claims that I am wrong that each session ID equates to a unique website visit. *See* Zervas Report ¶¶ 48-51. In fact, he was asked questions about sessions and session IDs at his deposition but describes these questions as "very deep philosophical question(s)." *See* Zervas Dep. at 200:18-201:9. He claims that I should have done testing or analysis and have no "technical basis" for my understanding of a session. *See* Zervas Dep. at 223:11-224:6. He also claims that there is no standard definition of a session and that I have no basis for correlating website visits with website sessions. *See* Zervas Dep. at 200:18-212:13.

28. I am surprised that Dr. Zervas would challenge whether there is a standard, well-known definition of a session. The knowledge academy, a global provider of training courses, provides an overview of how web developers typically define session ID[10]:

> A session ID, also known as a session token or session identifier, is a unique string of characters assigned by a web server when a user ***visits*** a website. This identifier allows the server to recognise and remember the user throughout their visit, which is referred to as a session.
> …
> Session ID works by helping a website recognise and remember users during their ***visit***. Since websites use HTTP or HTTPS, which are stateless and don't remember previous actions, Session IDs link all of a user's actions during a session. Here's how exactly it works:
>
> 1) User Connects to the Website: When a user ***visits a website***, the server will create a session. This happens immediately or after the user logs in.
>
> 2) Session ID is Created: The web server generates a unique Session ID for the user. Instead of using simple numbers, it is created with complex IDs with mixed letters, numbers, and symbols.

[10] Adams, Scarlett, *What is a Session ID? Everything You Need to Kno*w, the knowledge academy, November 4, 2025, https://www.theknowledgeacademy.com/blog/session-id, attached as **Exhibit I**.

> 3) Session ID is Sent to the Browser: The server sends the Session ID to the user's browser. It will be stored as a cookie. This ID identifies the user throughout the session.
>
> 4) Session ID is Sent Back with Every Request: For every new page or action, the browser sends the Session ID to the server. This allows the server to match the request with the correct session data, like login info, progress, or cart items.
>
> 5) Server Confirms and Responds: The server checks the Session ID to make sure it is valid. If it is, it completes the requested action, such as loading a page or processing a form.
>
> 6) Session Ends: The session ends when the user logs out, closes the browser, or is inactive for a while. At this point, the Session ID is invalidated, and the user must start a new session to continue.
>
> (Emphasis added).

29. Similarly, according to IONOS, a global web hosting and cloud services provider, "These session IDs allow a visitor to a website to be clearly identifiable during their ***visit to the site*** by way of an electronic tag granted by the server. Other terms for the session ID include session identifier and session token."[11] (Emphasis added).

30. According to SecureCoding, a company that provides webinars on how to build and maintain secure software products, a session ID is generally defined as follows[12]:

> A session ID, also known as a session token, is a unique number ID assigned by a website server to a specific user ***for the duration the user is on the website***. This session ID's storage is in the form of a cookie, form field, or URL. Each time a user opens a web browser and ***visits a website***, a session ID is generated. The session ID remains the same for some time. If a user closes the browser and reopens the web browser to visit a site, a new session ID is created again.
>
> (Emphasis added).

31. Meta chose to include `session_id` as a field in the `offsite_signals` table and

[11] IONOS Digital Guide, *What is a session ID?*, April 4, 2021, https://www.ionos.com/digitalguide/hosting/technical-matters/what-is-a-session-id, attached as **Exhibit J**.

[12] SecureCoding, *Session Management: An Overview*, April 29, 2021, https://www.securecoding.com/blog/session-management-an-overview, attached as **Exhibit K**.

defined it in its own data dictionary as "[t]he ID of the user session." *See* Zeidman Report ¶ 53, Ex. P.

32. As the sources above show, a session ID is equivalent to a website visit. Dr. Zervas claims that my "assumption that 'session_id' count equals the count of website visits is unsupported," Zervas Report ¶ 48, yet my definition of a session as a website visit is the one accepted by those of skill in the art of website development. While he asserts that Meta *may* use a different, non-standard definition, he does not provide what that different definition might be, despite ostensibly having access to Meta's internal workings as Meta's expert. There is no reason to think that the `session_id` in Meta's data is not synonymous with a visit to a website, and neither Meta nor Zervas has provided any evidence to the contrary.

33. Dr. Zervas states that, "From a technical perspective, there is no universally accepted definition for a website visit." Zervas Report ¶ 50. As I have shown in the above paragraphs, there is a universally accepted definition of a website session. A session is a commonsense definition of a website visit.

34. Dr. Zervas describes how a session may time out after a certain number of seconds of inactivity by the user, and thus be recorded as multiple sessions, even though Dr. Zervas claims this would only represent a single "visit" by the user. *See* Zervas Report ¶¶ 50-51. But in my experience, as a session is typically defined, when a session ends after a time period of inactivity, the user must log in again. This is necessary for security purposes so that if a user steps away from a computer, another user cannot obtain the first user's private information. Based on my experience and expertise, I believe that if a user is inactive for a period of time and needs to log back into the website again, that should be considered two separate visits to the site, particularly since the user would need to enter a username and password, at which point information would again be sent to Meta via the Meta Pixel.

35. Dr. Zervas also contends that I did not provide any evidence that Meta defines `session_id` in a way that corresponds to a website visit. *See* Zervas Report ¶ 52. However, the standard definition of a session corresponds to the commonsense concept of a website visit.

36. Meta argues that I "fail[ed] to match a 'visit' to a human user… and made no attempt to match 'visits' to putative class members, even though [I] acknowledged that putative class members, particularly those who disclosed any sensitive data, may well have made multiple visits." Mot. at 20. The Motion goes on to claim that I "admitted that there are numerous ways that a 'session ID' might count a single visit multiple times." Mot. at 20. This misconstrues my actual testimony. The questions Meta asked me during that portion of my deposition focused on how the counting of visits would be affected by users visiting a site either (a) simultaneously from two different browsers on the same computer; (b) simultaneously from two different devices; or (c) during a brief disconnection from the Internet.

37. The Motion then inaccurately concludes that I "conceded that 'each unique session ID' may not in fact 'represent[] a unique visit to the [] websites.'" Mot. at 20. I made no such concession in responding to these questions, and these quotations are taken from my opening report, which I did not contradict at my deposition as implied in Meta's Motion. Instead, after being asked the above hypothetical questions, and after answering them, I simply stated that I did not know how visits were affected during these hypothetical situations. *See* Zeidman Dep. at 181:14-182:5. I did not concede anything about session IDs and unique visits. In fact, I was only asked twice about whether these hypothetical situations would be counted as one or two visits, and I answered that I would need to research that. In fact, during the part of the transcript that is referenced, I was never asked about session IDs, and I made no statements about them.

38. Notably, neither Meta nor Dr. Zervas identifies a single example—despite reviewing the same produced dataset—where session_id changed during active browser interaction or remained constant across a long inactivity gap. In fact, Dr. Zervas conceded at deposition that he had not conducted any analysis to identify such examples. *See* Zervas Dep. at 205:15-206:20, 209:6-20.

39. In fact, Meta's other expert, Steven Tadelis, discusses sessions, session IDs, visits, and visitors in detail in **Section B** of his report, "Analyses of the Offsite Signals Data Show That a Substantial Portion of Sessions on the H&R Block and TaxAct Websites Were Consistent with

Misclicks or Quickbacks." *See* Rebuttal Expert Report of Steven Tadelis ("Tadelis Report") ¶¶ 23-29. Professor Tadelis treats each `session_id` as a separate session corresponding to a single user visit. He repeatedly analyzes "sessions," "session durations," and "session-level characteristics" using `session_id` to define a session. He treats each `session_id` as a distinct unit of user interaction with the website for purposes of analyzing "quickbacks," "misclicks," and "session length." Tadelis Report at 11-15. Professor Tadelis's analysis aligns directly with my approach, as he discusses what data is sent to Meta for each session, regardless of the duration of the session, and associates each session with a single visit to the website. *See* Tadelis Report at ¶¶ 23-29. His notes in his report below Figure 2 on page 13 explain how each specific session has a unique `session_id` variable value associated with it. *See* Tadelis Report Fig. 2 ("Sessions are counted by unique values of the variable session_id . . . .").

b. Meta's Data Allows for the Exclusion of Visits to the H&R Block and TaxAct Websites By Non-Humans

40. Non-humans (i.e., bots) are not members of the classes. The Hive data has a data field that indicates whether the visitor was a bot, so obviously Meta has ways to separate humans from non-humans. Regardless of how Meta determines this, one can use the Hive data and the bot indicator to eliminate those visits by non-humans. I created and ran a SQL query on the Meta Hive database to determine the number and percentage of discarded entries because Meta determined that the entries came from bots.[13] Bots are automated accesses to websites that were not human users. The discarded events can be found in the offsite_signals table when the [redacted] field has the value discarded. In that same table is a field called [redacted] that can contain the value `bot_traffic`, meaning that Meta determined that it came from a bot rather than a human. *See* **Exhibit M** (excerpt of transcript of April 1, 2025 Deposition of Abhinav Anand in Meta Healthcare action) at 98:15-22 (Meta "identif[ied] [bot] traffic. And then dropp[ed] data

[13] SQL code attached as **Exhibit L**.

based on that"); **Exhibit N** (excerpt of errata sheet correcting "bought" to "bot").

41. Table 1 below shows the results of the query. The number of discarded events can be filtered from the Hive data, and then the specific number of events due to bots can be further filtered. This also shows that the percentage of total discarded bot events ranges, by sample date, from 0% to 2.02%, with a daily average of 0.35%.

ds	Entity	Total events	Used in prod events	Pct used in prod events	Discarded events	Pct discarded events	Discarded bot events	Pct discarded bot events
7/26/2022	hrblock	3066682	1919163	62.58	1147519	37.42	17579	0.57
8/26/2022	hrblock	2255583	1426776	63.26	828807	36.74	42246	1.87
9/26/2022	hrblock	2178970	1413571	64.87	765399	35.13	27408	1.26
10/26/2022	hrblock	2694163	1723485	63.97	970678	36.03	33992	1.26
11/26/2022	hrblock	1472860	963619	65.43	509241	34.57	29737	2.02
12/26/2022	hrblock	615747	615673	99.99	74	0.01	0	0
1/26/2023	hrblock	10625967	10620609	99.95	5358	0.05	0	0
2/26/2023	hrblock	6686174	6676213	99.85	9961	0.15	0	0
3/26/2023	hrblock	5449358	5446598	99.95	2760	0.05	0	0
4/26/2023	hrblock	1579819	1579236	99.96	583	0.04	0	0
7/26/2022	taxact	151754	142538	93.93	9216	6.07	0	0
8/26/2022	taxact	120194	107678	89.59	12516	10.41	0	0
9/26/2022	taxact	147074	141617	96.29	5457	3.71	0	0
10/26/2022	taxact	128712	123826	96.2	4886	3.8	0	0
11/26/2022	taxact	60836	60836	100	0	0	0	0
12/26/2022	taxact	56270	54709	97.23	1561	2.77	0	0
1/26/2023	taxact	1630	1630	100	0	0	0	0
2/26/2023	taxact	147	147	100	0	0	0	0
3/26/2023	taxact	134	134	100	0	0	0	0
4/26/2023	taxact	305	305	100	0	0	0	0

Table 1. Discarded events

ii. *It is Irrelevant That My Proposed Method for Counting Visits to the H&R Block and TaxAct Websites Cannot Be Used to Exclude Visits from Users Who Provided Consent*

42. I understand that whether users of the H&R Block and Tax Act websites consented to the Meta Pixel's collection and transmission of data to be a legal issue, not a technical issue, and thus I do not address it.

iii. *My Proposed Method for Counting Visits to the H&R Block and TaxAct Websites Can Be Used to Count Visits from Individuals in California*

43. Dr. Zervas claims that my proposed methodologies for counting visits to the H&R Block and TaxAct websites cannot be used to count visits from individuals in California. Yet it is certainly and obviously possible to count visits from California users, because the Meta Hive data includes what Meta has identified as tending to be the zip code of the visitor's device's IP address, which can be easily correlated to a city and state. *See* **Exhibit O** (excerpt of transcript of April 28, 2025 30(b)(6) Deposition of Tobias Wooldridge in Meta Healthcare action) at 107:2-108:2; *see, e.g.*, **Exhibit G** (defining geo_ip_zip as "[t]he zip code where the pixel is fired"). Thus Meta is able to determine that information, and we can utilize that same information.

44. I have written a SQL script to extract this information[14] from the Meta Hive database by (a) taking the zip code in the `geo_ip_zip` field of the `ads_pixel_traffic` table of the Meta Hive database; (b) searching for the corresponding state in the `physical_state` field of the publicly available US Post Office database `usps`[15]; and (c) only recording those events with zip codes in California. I also use the field [redacted] to match these zip codes to particular Meta users and remove duplicates where one user had

[14] SQL code attached as **Exhibit P.**

[15] ZIP_Locale_Detail.xlsx available at https://postalpro.usps.com/ZIP_Locale_Detail.

multiple sessions during this period. Using this script to extract California users from the `ads_pixel_traffic` table of the Meta Hive, I have found 61,860 unique users from California, 14,991 from TaxAct and 46,869 from H&R Block. Because Meta chose to generate and store ZIP-level location data for each session, it is reasonable and appropriate to use that same data to count how many visits Meta recorded as originating from California. My methodology therefore counts visits as Meta itself classified them, rather than attempting to determine location independently.

C. My Proposed Method Counts Website Visits to the H&R Block and TaxAct Websites not Website Visitors

45. Dr. Zervas criticized my "proposed methodologies"[16] on the basis that I cannot "accurately identify visitors to the H&R Block and TaxAct websites during the proposed class periods." Zervas Report ¶ 62. He then describes, in ¶ 63 through ¶ 68, his alleged issues with my method. However, I never claimed that my method counted *visitors*; it counts *visits*. The proposed method counts the number of times that these websites were visited and sent information to Meta. The section header in my report on page 14 clearly states, "Calculating ***Visits*** to the Tax Preparer Websites." (Emphasis added.) I also clearly state that "If this visitor comes back to the website again at a later time, that would be considered a second visit." Zeidman Report ¶ 51.

46. Dr. Zervas' criticisms of my method in his report, and Meta's in its Motion, for purportedly failing to calculate visitors are moot because they attack a method I never actually proposed.

47. Dr. Zervas states that one visitor may have many unique encrypted IP addresses and thus I cannot use these encrypted IP addresses to determine the number of visitors from California. *See* Zervas Report ¶ 63. It is true that a user may have more than one encrypted IP address. However, as I stated in my report, my purpose for referring to the encrypted IP addresses was solely to show that the H&R Block and TaxAct websites during the proposed class periods

[16] I have proposed methods, not methodologies, which are collections of methods.

were visited by more than 40 people each, both nationally and from California specifically. *See* Zeidman Report ¶ 43. Even though each new session might have a unique encrypted IP address, assuming an unreasonable number of 270 visits per person (the number of unique encrypted IP address values Meta says it found for Plaintiff Jane Doe, *see* Mot. at 15-16), dividing the number of unique encrypted IP addresses by 270 shows 55 unique visitors from TaxAct and 173 unique visitors from H&R Block in *just* the limited sample of data produced by Meta.

D. My Opinion that I Found an "Enormous Amount of Tax Information" and Other Data Transmitted to Meta is Correct

48. In my report, I stated, "I… found there was an enormous amount of tax information and other data transmitted to Meta from the Tax Preparers' websites." *See* Zeidman Report ¶ 57.2. I was not asked to quantify the amount of tax information that was transmitted but simply made a qualitative description of the amount. I can certainly go back to the original data and quantify the amount of tax information and other data transmitted to Meta, and I have done so here.

49. Meta's Motion discusses my characterization of the data as "enormous" five times, asserting that I made no attempt to quantify the data. *See* Mot. at 2, 16, 17, 18.

i. *My Opinions Do Not Contain Methodological Flaws*

50. As I explained above, I used a commonsense definition of tax information as information that I would expect to be found on a tax form. Because I had limited information about the data that Meta had provided, I had to make assumptions about what each piece of data represented based on the name of the data field. My assumptions are reasonable because the names of the data fields closely align to common fields required in tax forms.

51. Dr. Zervas claims that my assertions are wrong about which data fields represent tax information even though he himself does not provide a definition of "tax information," which makes his assertions no more valid than mine. *See* Zervas Report ¶¶ 69-77. He chooses just one example of a data field among many in the data, `NumChildButtons`, to claim that my

understanding is wrong. *See* Zervas Report ¶¶ 72. He states that "Mr. Zeidman ignored that in web development, 'child' is the standard technical term for an element nested inside another 'parent' element." Zervas Report ¶¶ 72. Dr. Zervas correctly describes child and parent web elements. However, a "child" is also the biological offspring of a grown adult, referred to as a "parent." Dr. Zervas cites to no Meta-specific sources to conclude that his description is what `NumChildButton` actually captures. His criticism is purely speculation.

52. Meta's Motion makes the same assertion about this same data field. Meta claims to know exactly what this data field represents but then provides only speculation. Mot. at 17. Given that Meta created the Meta Pixel, I would expect that Meta might be able to produce documentation about the `NumChildButtons` data field that I could not find, but even Meta provides no specific information other than speculation.

53. There is no reason to believe that Dr. Zervas's assumption concerning the "child" field is more accurate than mine, and there are several reasons to conclude the contrary. First, I can find no references online, other than descriptions of Meta Pixels, that reference `NumChildButtons`, so at the very least it is not a common data field used for information about nested folders. Second, if this data field represents a hierarchy of button elements, I can think of no reason that such data would be sent to Meta or anywhere else. This would be analogous to mailing a letter that was simply an envelope ("child") inside another envelop ("parent"). Or sending an email with the content "This is an email." Third, the other examples that I give, which Dr. Zervas does not address, are called `num_of_dependents`, `w2`, `agi`, `federal_owe_amount`, and `federal_refund_amount`, which common sense indicates comprise tax information.

ii. *My Review Shows That the Event Data I Analyzed Appears Frequently*

54. I created two SQL queries, one to count each time tax information was sent to Meta in a JSON file that was recorded in the offsite_signals table in the Meta Hive, and one to count

those times where it was populated with a number (i.e., not blank and not removed).[17] Specifically, I considered the following information, among others, as tax information:

1. age_range
2. agi
3. charitable_contribution
4. f1099misc
5. federal_owe_amount
6. federal_refund_amount
7. federal_revenue
8. filing_status
9. investments
10. return_year
11. rpt_revenue
12. schedule_c
13. standard_deduction
14. state_revenue
15. svc_revenue
16. tax_form
17. total_revenue
18. w2

[17] SQL code attached as **Exhibit Q**.

55. I found that the sample Hive data produced in this litigation had 19,519 events where the above tax information was transmitted to Meta in some form, and 12,227 times that this tax information was transmitted and was not blank and/or filtered. In my opinion, this is a large amount of tax information in just the sample data produced by Meta. And when expanded across the entire class periods, it is reasonable to characterize it as an "enormous" amount of tax information.

E. I Did Not Fail to Consider Variability Due to Developer and User Controls

56. Dr. Zervas explains that there exist various controls that could prevent or limit Meta Pixel data from being sent to Meta, including browser-level tools such as ad blockers or cookie restrictions, private browsing modes, and developer-side options to disable Automatic Events. *See* Zervas Report ¶¶ 81-112. I do not dispute that these controls exist. However, the relevance of these controls depends on whether they were actually used. The fact that the events at issue appear in Meta's Hive data demonstrates that, for the sessions reflected there, those controls were not effective and/or not enabled. More importantly, these controls are no longer relevant because, as I have been informed by the plaintiffs' attorneys, the proposed classes now only include individuals whose data was actually received and stored by Meta.

57. In addition, the publicly available HAR files for H&R Block and TaxAct analyzed by independent journalists show that Automatic Events such as SubscribedButtonClick and Microdata events were automatically transmitted from users' browsers to Meta without requiring custom developer code.[18] These same types of Automatic Events appear in the Hive datasets produced by Meta. This provides further evidence that Automatic Events were in fact sent to Meta for the sessions reflected in the data I analyzed. My opinions are therefore based on what Meta actually received and recorded, not on theoretical controls that, if enabled, would have prevented

[18] the-markup / meta-pixel-taxes, *GitHub*, https://github.com/the-markup/meta-pixel-taxes/ (November 21, 2022).

the data from appearing in Meta's own systems.

F. Meta's Detection and Filtration Code is Irrelevant, as are User Controls

58. I have been informed by counsel to the Plaintiffs that the classes are now defined by those users whose data is in Meta's Hive tables. Because this necessarily only includes users whose data was not filtered by Meta's detection code or blocked by user interventions, these criticisms are irrelevant.

G. I Did Not Mischaracterize the Technical Nature of the Alleged Pen Register Data

59. Dr. Zervas describes a test whereby he removed pen register data from the headers of the web page at hrblock.com and showed that removing such data did not stop the page from "loading successfully" and did not stop the Meta Pixel from transmitting data to Meta. *See* Zervas Report ¶ 122. This test provides no insight into the function of this header data. First, although he could see the web page at H&R Block, how can he determine that it "loaded successfully." Dr. Zervas does not explain what he means by this term. Does he mean that it looks correct to a user? That it looks mostly correct with minor layout issues? That it functions correctly in some aspects? In all aspects? He does not explain how he determined that a page "loaded successfully."

60. Web browsers are designed to be very fault tolerant because the Internet is a very unreliable communication system. Data is often lost during transmission, but web browsers are designed to fill in information from their local cache containing page elements from previous visits and also to fill in any obviously missing elements by guessing what that element might be. For example, if a table is transmitted with an opening <table> tag but no closing </table> tag, the browser will guess at the most logical place for that closing tag to be and draw a closed table. Dr. Zervas does not explain how he determined that the page "loaded successfully."

61. More importantly, just because the Meta Pixel works when this information is missing, this data appears in the Meta Hive, which indicates that the data is transmitted when it is

not missing. In other words, during normal web browsing this data is included as part of normal addressing and routing information, and it is collected and transmitted by the Meta Pixel.

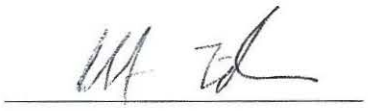
62. Meta claims that I "did not actually examine whether the Meta Pixel code enables the transmission of 'information such as IP address or a ZIP code or a city or a state." Mot. at 14. Similarly, Dr. Zervas states that some of the data that I have identified is not directly transferred to Meta but rather inferred from data that is transmitted to Meta. *See* Zervas Report ¶ 123. Dr. Zervas therefore concludes that it is not pen register data according to the statutes. As I note above, The data produced by Meta includes tables with fields clearly marked as "city," "country," "geo_ip_zip," and IP addresses. I understand the distinction between transmitted data and inferred data to be a legal issue, not a technical issue, and thus I do not address it.

V. CONCLUSIONS

63. In this report, I respond to the criticisms raised by Meta and its experts, Dr. Zervas and Professor Tadelis. I am well-qualified to opine on the matters in my original report and in this reply. My opinions are based on reliable methods supported by my experience and standard industry practices. Any criticisms are either unfounded or are easily addressed by minor clarifications regarding my approach.

64. It is my understanding that discovery in this case is ongoing. Accordingly, I reserve the right to supplement or amend my opinions in light of any additional evidence, testimony, or information that may be provided to me after the date of this report. I also reserve the right to supplement or amend my opinions in response to any expert reports served by any other party in the lawsuit.

Dated: December 15, 2025



Robert Zeidman

Index of Exhibits

1. Exhibit A: GeeksforGeeks, TCP/IP Model, https://www.geeksforgeeks.org/computer-networks/tcp-ip-model
2. Exhibit B: Maxmind, "Geolocation accuracy" https://support.maxmind.com/knowledge-base/articles/maxmind-geolocation-accuracy
3. Exhibit C: James Sanders, "IP Geolocation in 2025: A Comprehensive Guide to Location Intelligence," litport, https://litport.net/blog/ip-geolocation-a-comprehensive-guide-to-location-intelligence-69228
4. Exhibits D: ad_pixels_traffic table
5. Exhibit E: offsite_signals table
6. Exhibit F: offsite_signals_pipe table
7. Exhibit G: PIXEL_TAX000058898-905
8. Exhibit H: Thales Cybersecurity, HTTP/2, https://www.imperva.com/learn/performance/http2
9. Exhibit I: Adams, Scarlett, What is a Session ID? Everything You Need to Know, the knowledge academy
10. Exhibit J: IONOS Digital Guide, What is a session ID?, April 4, 2021, https://www.ionos.com/digitalguide/hosting/technical-matters/what-is-a-session-id
11. Exhibit K: SecureCoding, Session Management: An Overview, April 29, 2021, https://www.securecoding.com/blog/session-management-an-overview
12. Exhibit L: SQL Code-Discarded Entries
13. Exhibit M: Transcript of Deposition of Abhinav Anand in Meta Healthcare

14. Exhibit N: Errata Sheet for Transcript of Deposition of Abhinav Anand in Meta Healthcare

15. Exhibit O: 30(b)(6) Deposition of Tobias Wooldridge in Meta Healthcare

16. Exhibit P: SQL Code-Visits

17. Exhibit Q: SQL Code-Tax Information & Populated by Number

EXHIBIT A

TCP/IP Model

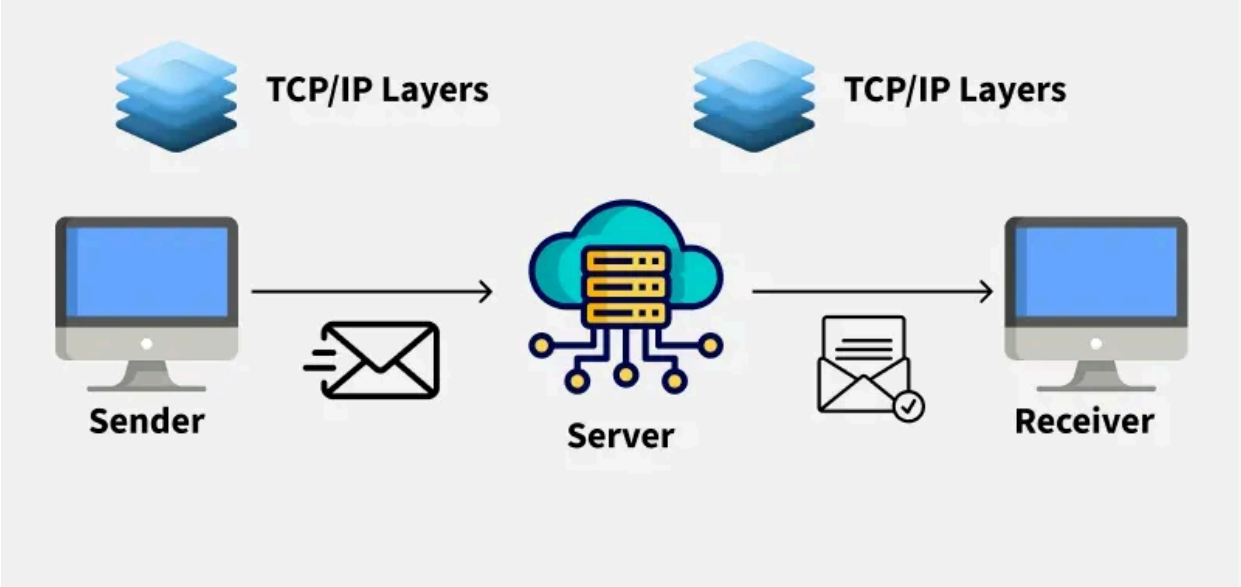
Last Updated : 10 Dec, 2025

The TCP/IP model is a framework that is used to model the communication in a network. It is mainly a collection of network protocols and organization of these protocols in different layers for modeling the network.

- It has five layers: Application, Transport, Network/Internet, Data link layer, Physical layer
- While the OSI model has seven layers, the 5 layer TCP/IP model is simpler and commonly used in today's Internet and networking systems.

Role of TCP/IP

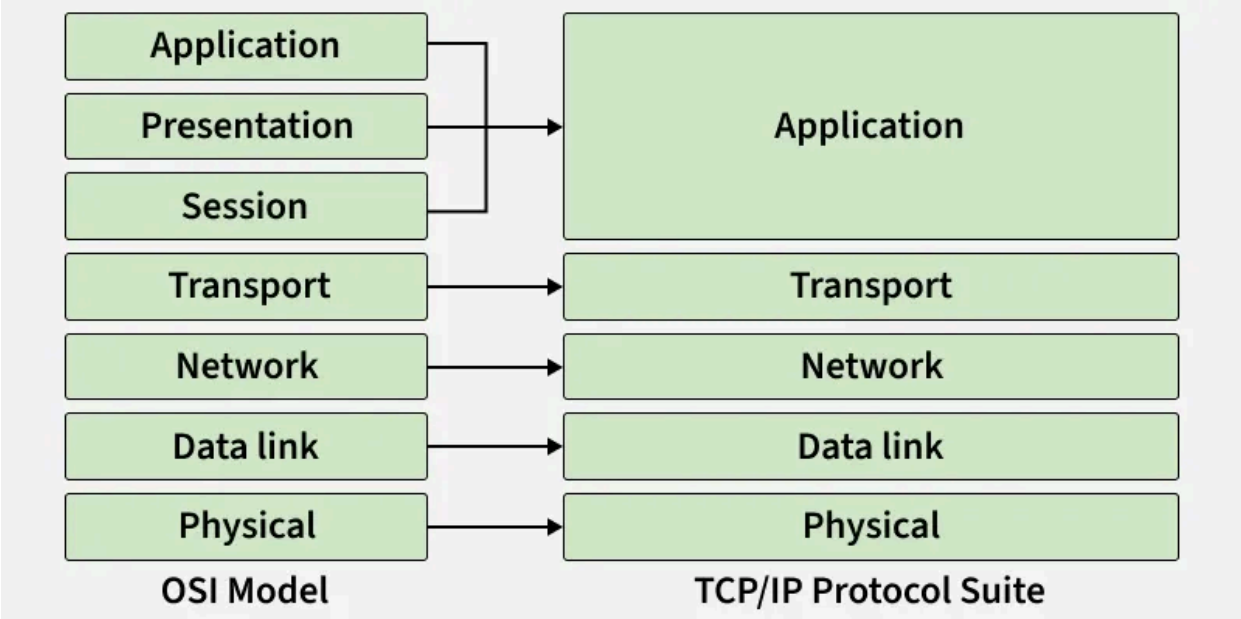
One of its main goals is to make sure that the data sent by the sender arrives safely and correctly at the receiver's end. To do this, the data is broken down into smaller parts called packets before being sent. These packets travel separately and are reassembled in the correct order when they reach the destination.



TCP/IP

> ***Note:*** *This helps prevent errors and makes sure the message is complete and accurate.*

Layers of TCP/IP Model



Layer's of Tcp Model

1. Application Layer

The Application Layer is the top layer of the TCP/IP model and the one closest to the user. This is where all the apps you use like web

browsers, email clients, or file sharing tools connect to the network.

- It acts like a bridge between your software (like Chrome, Gmail, or WhatsApp) and the lower layers of the network that actually send and receive data.
- It supports different protocols like HTTP (for websites), FTP (for file transfers), SMTP (for emails), and DNS (for finding website addresses).
- It also manages things like data formatting, so both sender and receiver understand the data, encryption to keep data safe, and session management to keep track of ongoing connections.

2. Transport Layer

The Transport Layer is responsible for delivering data accurately, reliably, and in the correct order between two devices communicating over a network. Whenever you send something—like a message, file, video, or webpage request—the transport layer ensures it reaches the other side properly.

This layer mainly uses two protocols: TCP and UDP, depending on whether the communication needs to be more reliable or more fast.

TCP (Transmission Control Protocol)

TCP is used when data must be **error-free, complete, and in order**. Examples: loading websites, downloading files, sending emails.

TCP features:

- Checks for errors in data
- Resends lost or damaged data
- Ensures everything arrives in the right order
- Provides reliable, connection-oriented communication

This makes TCP slower but **very accurate**.

UDP (User Datagram Protocol)

UDP is used when **speed is more important than perfect accuracy**. Examples: live streaming, online gaming, VoIP calls.

UDP features:

- No error checking
- No retransmission of lost data
- No guarantee of order
- Fast and lightweight

This makes UDP much faster, but **less reliable** than TCP.

3. Network Layer

The Internet Layer is used for finding the best path for data to travel across different networks so it can reach the right destination. It works like a traffic controller, helping data packets move from one network to another until they reach the correct device.

- This layer uses the Internet Protocol (IP) to give every device a unique IP address, which helps identify where data should go.
- The main job of this layer is routing deciding the best way for data to travel.
- It also takes care of packet forwarding (moving data from one point to another), fragmentation (breaking large data into smaller parts), and addressing.

4. DataLink Layer

- The Internet is formed by multiple links (LANs & WANs) connected through routers.
- Routers decide the best path for datagrams to reach the destination.
- Different links may use different protocols at the data-link layer.
- TCP/IP does not specify any single data-link protocol — it supports all standard & proprietary ones.

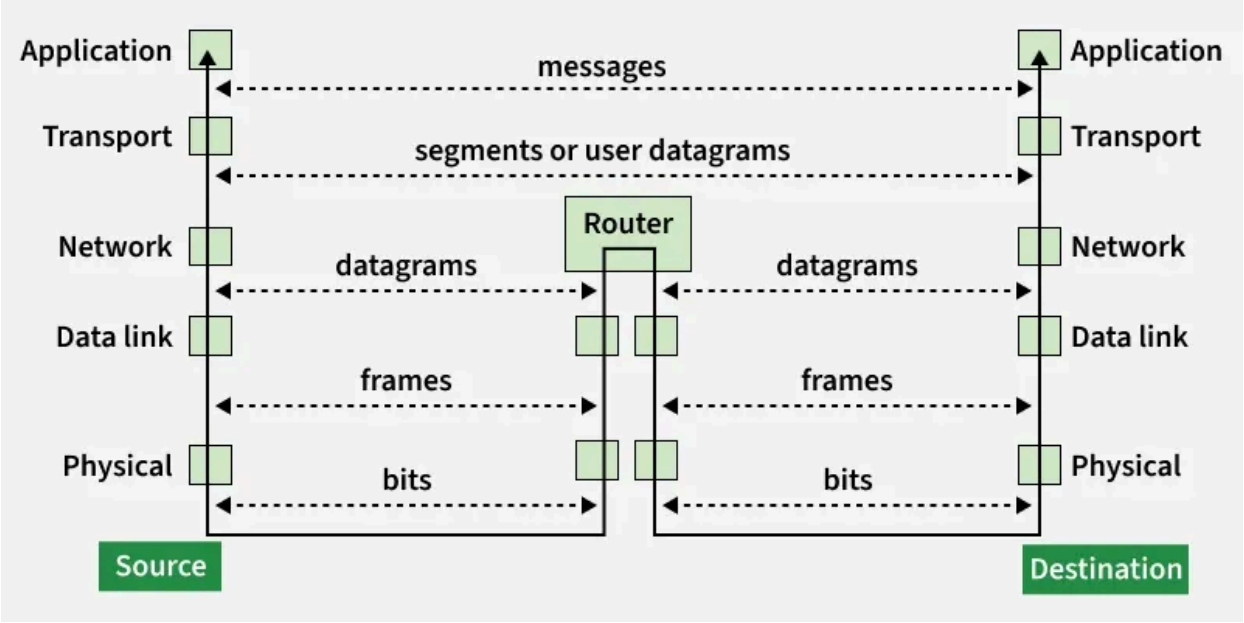
- The data-link layer encapsulates the datagram into a frame for transmission.
- Link-layer services differ:
  - Some provide error detection & correction
  - Some provide only error detection
  - Others may offer minimal or no error control

5. Physical Layer

- Responsible for transmitting individual bits of a frame across a link.
- It is the lowest layer in the TCP/IP protocol suite.
- Communication at this layer is logical, because:
  - A transmission medium (like cable or air) exists below it.
- The transmission medium does not carry bits directly — it carries:
  - Electrical signals (wired media)
  - Optical signals (fiber-optic)
  - Radio waves (wireless)
- Bits from the data-link layer are converted into signals for transmission.
- At the receiver side, signals are converted back to bits.

Working of TCP/IP Model

The working of TCP/IP can be explained with the help of the diagram given below and explained :



tcp/ip Model

When Sending Data (From Sender to Receiver)

- **Application Layer**: Prepares user data using protocols like HTTP, FTP, or SMTP.
- **Transport Layer (TCP/UDP)**: Breaks data into segments and ensures reliable (TCP) or fast (UDP) delivery.
- **Internet Layer (IP)**: Adds IP addresses and decides the best route for each packet.
- **Link Layer (Network Access Layer)**: Converts packets into frames and sends them over the physical network.

When Receiving Data (At the Destination)

- **Link Layer**: Receives bits from the network and rebuilds frames to pass to the next layer.
- **Internet Layer**: Checks the IP address, removes the IP header, and forwards data to the Transport Layer.
- **Transport Layer**: Reassembles segments, checks for errors, and ensures data is complete.

- **Application Layer**: Delivers the final data to the correct application (e.g., displays a web page in the browser).

Why TCP/IP is Used Over the OSI Model

TCP/IP is used over the OSI model because it is simpler, practical, and widely adopted for real-world networking and the internet. The diagram below shows the comparison of OSI layer with the TCP:

Reason	Explanation
Simpler Structure	TCP/IP has only 5 layers, compared to 7 in OSI, making it easier to implement and understand in real systems.
Protocol-Driven Design	TCP/IP was designed based on working protocols, while the OSI model is more of a theoretical framework.
Flexibility and Robustness	TCP/IP adapts well to different hardware and networks and includes error handling, routing, and congestion control.
Open Standard	TCP/IP is open, free to use, and not controlled by any single organization, helping it gain universal acceptance.
Actual Use vs Conceptual Model	The OSI model is great for education and design principles, but TCP/IP is the one actually used in real-world networking.

Advantages of TCP/IP Model

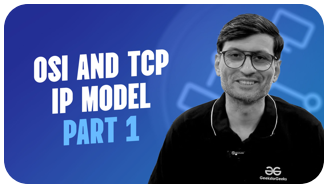
- **Interoperability** : The TCP/IP model allows different types of computers and networks to communicate with each other, promoting

compatibility and cooperation among diverse systems.

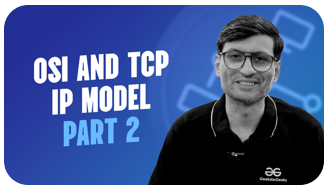
- **Scalability** : TCP/IP is highly scalable, making it suitable for both small and large networks, from local area networks (LANs) to wide area networks (WANs) like the internet.
- **Standardization** : It is based on open standards and protocols, ensuring that different devices and software can work together without compatibility issues.
- **Flexibility** : The model supports various routing protocols, data types, and communication methods, making it adaptable to different networking needs.
- **Reliability** : TCP/IP includes error-checking and retransmission features that ensure reliable data transfer, even over long distances and through various network conditions.

Disadvantages of TCP/IP Model

- **Security Concerns** : TCP/IP was not originally designed with security in mind. While there are now many security protocols available (such as SSL/TLS), they have been added on top of the basic TCP/IP model, which can lead to vulnerabilities.
- **Inefficiency for Small Networks** : For very small networks, the overhead and complexity of the TCP/IP model may be unnecessary and inefficient compared to simpler networking protocols.
- **Limited by Address Space** : Although IPv6 addresses this issue, the older IPv4 system has a limited address space, which can lead to issues with address exhaustion in larger networks.
- **Data Overhead** : TCP the transport protocol, includes a significant amount of overhead to ensure reliable transmission.



OSI and TCP IP Mode (Part 1)



OSI and TCP IP Mode (Part 2)

OSI and TCP IP Model (Part 1)

Visit Course

Comment

A achivc... + Follow 624

Article Tags : Misc Computer Networks GATE CS

Explore

Computer Network Basics

Physical Layer

Data Link Layer

Network Layer

Transport Layer

Session Layer & Presentation Layer

Application Layer

Advanced Topics

Practice

GeeksforGeeks
Sanchhaya Education Private Limited

Corporate & Communications Address:

A-143, 7th Floor, Sovereign Corporate Tower, Sector- 136, Noida, Uttar Pradesh (201305)

Registered Address:

K 061, Tower K, Gulshan Vivante Apartment, Sector 137, Noida, Gautam Buddh Nagar, Uttar Pradesh, 201305

EXHIBIT B

Geolocation accuracy

One of our greatest priorities is to keep our data as accurate as possible. In cases where it's not possible to be as accurate as we would like, we are transparent with our customers about technological and other limitations.

Limitations to IP geolocation

It is not possible for us to guarantee 100% geolocation accuracy. Accuracy exhibits high variability according to country, distance, type of IP (cellular vs. broadband, IPv4 vs. IPv6), and practices of ISPs. We do not guarantee exact matches to our competitors' data, nor identical accuracy to theirs, as we may use different data providers in some instances.

Pricing for GeoIP Products and Services

Account and purchasing ›

Data privacy ›

It is also important to note that GeoIP geolocation data is never precise enough to identify or locate a specific household, individual, or street address.

Some times, even for IP addresses we can geolocate quite well, we cannot geolocate the person who is using the IP address. For example, if someone is using an anonymizing proxy like a VPN, or someone is hosting a web site, we may be able to geolocate the web server being used to run the VPN or host the web site, but we will not be able geolocate the end-user or the business associated with the web site. Learn more about anonymizer and proxy detection in GeoIP products and services.

If you would like to learn more, we have a blog post explaining some of the technological issues and limitations for IP geolocation accuracy.

Overview of GeoIP geolocation accuracy

With those limitations in mind, we estimate that our GeoIP products can identify users at the country level with 99.8% accuracy. For IPs located within the U.S., we estimate around an 80% accuracy at the state/region level, and a 66% accuracy for cities (within a 50km radius of that city). Learn more about geolocation areas (our accuracy radius) and how to use it on our blog.

You can get more information about the accuracy of our IP geolocation data for other countries using the GeoIP City accuracy page on our main website.

Variations in geolocation accuracy

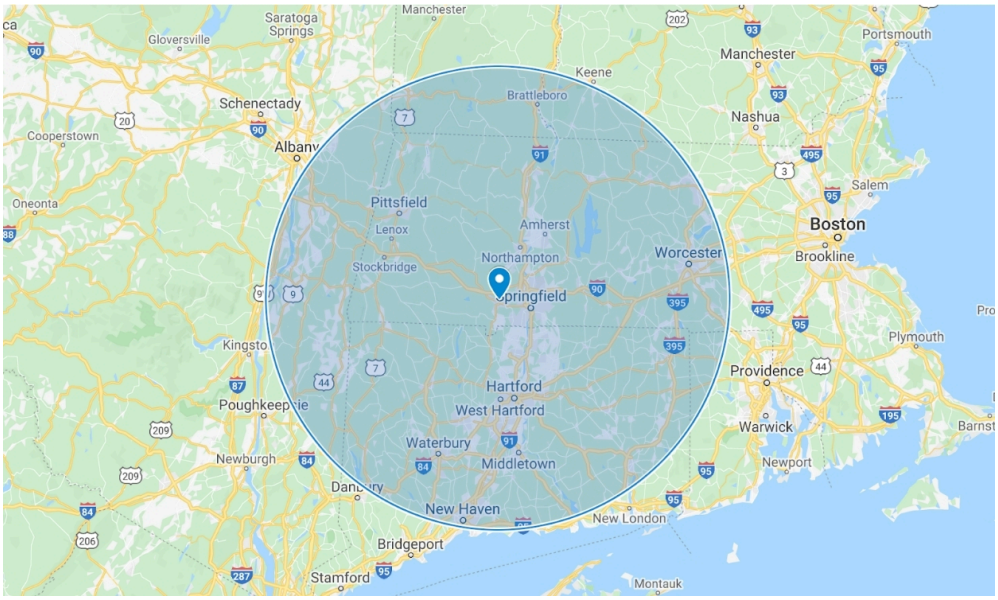
Some IP addresses cannot be located with the same accuracy as others. For example, IP addresses used in mobile networks may be used by mobile phones across a large distance. Other IP addresses may be used as part of a business VPN or consumer privacy network, so the end-user may be anywhere within a region, but more specific geolocation is not possible.

Learn more about business VPNs and consumer privacy networks.

In cases where we cannot geolocate an IP address with a high level of specificity, we will not include more granular data. For example, if an IP address is part of a mobile used across the state of Massachusetts in the United States, we would include continent, country, and subdivision (state) data for the IP address, but we would not include city or postal code data. You should set up your integration with GeoIP products and services to fall back on less-specific geolocation data when more specific data is not available.

Accuracy radius

In our geolocation products with city-level geolocation data, we will also include an accuracy radius, to give you a sense of how accurate our geolocation is for that IP address.



In the example above, GeoIP products and services return the coordinates 42.1293, -72.7522 with an accuracy radius of 100km. The actual geolocation of the IP address is likely within the 100km-radius circle shown above.

Geolocation confidence

Some of our geolocation products also include confidence factors. Confidence factors are our confidence, expressed as a percent, that our geolocation values are correct. We provide confidence factors for the country, city, subdivisions, and postal code values in our GeoIP Enterprise database and our GeoIP Insights web service.

You can use confidence factors to build more powerful geolocation responses, using fallback value of less granular geolocation data when the geolocation confidence falls below a certain threshold. For example, if the confidence for city-level location for an IP lookup fell below 50, you could design your integration to use the subdivision-level location value instead.

Our developer portal has specifications for our confidence factors:

- Read the database specifications for our confidence factors on our developer portal.
- You can read the API specifications for our confidence factors on our developer portal:
  - `/country/confidence`
  - `/city/confidence`
  - `/subdivision/confidence`
  - `/postal/confidence`

Keeping your data accurate

If you use databases rather than web services, you should download database updates as they are released in order to make sure you have the most accurate geolocation data possible. Learn more about updating databases. All database customers and users are required to maintain up to date databases as part of their license agreement. Learn more the requirements for keeping data up to date.

Web services customers will always have access to our most accurate data.

Problems with our IP geolocation data

> In almost all cases, MaxMind follows ISO to determine which country a particular subdivision belongs to, even in cases where a region is disputed. When alternative country assignments are available under ISO, MaxMind's decision about country association is not based on any political position.

Our data team works hard to keep our data accurate. We are always glad to review IPs to ensure our accuracy is as close to perfect as we can get it. Please reach out to our support team if you have questions about a particular IP address. You can also submit a data correction request.

Was this article helpful? Yes No

Submit a data correction

Your privacy choices

Notice of collection

Company

About

Contact us

Terms of Use | Privacy Policy

EXHIBIT C

IP Geolocation in 2025: A Comprehensive Guide to Location Intelligence

published 2025-05-23 by James Sanders 4,346 views

Key Takeaways

- IP geolocation pinpoints a device's geographical location based on its IP address, accurate to country (99%), region (95%), and city (80-90%) levels
- Modern geolocation combines IP-based, device-based, and contextual data for enhanced accuracy and business intelligence
- Businesses leverage location data for personalization, fraud detection, compliance, and marketing optimization
- Privacy concerns are driving new regulations and technologies that balance location benefits with user control
- The future of geolocation is moving toward hybrid models that respect privacy while enabling personalization

What is IP Geolocation?

IP geolocation is the process of determining the geographical location of an internet-connected device based on its IP address. This technology maps the digital world to physical locations, providing valuable context for businesses and services online.

Unlike GPS, which requires hardware in your device and explicit permission, IP geolocation works behind the scenes and provides a general area rather than an exact location. It can reveal details such as:

- Country and continent
- Region, state, or province
- City
- Postal or ZIP code
- Approximate latitude and longitude
- Time zone
- Connection type and speed
- Internet Service Provider (ISP)

How IP Geolocation Technology Works

Understanding IP geolocation requires first grasping what IP addresses are and how they're distributed.

The IP Address System

IP addresses function as the internet's addressing system - digital equivalents of postal addresses that enable devices to find and communicate with each other online. These addresses aren't randomly assigned but follow a structured allocation process:

1. The Internet Assigned Numbers Authority (IANA) allocates large IP address blocks to Regional Internet Registries (RIRs)
2. RIRs like ARIN (North America), RIPE NCC (Europe), and APNIC (Asia-Pacific) distribute smaller blocks to National or Local Internet Registries

3. These registries allocate addresses to Internet Service Providers (ISPs)
4. ISPs assign individual IP addresses to end users

This hierarchical distribution creates geographical patterns that geolocation services can analyze. For more detailed information about the differences between IP versions, check out our guide on IPv4 vs IPv6 differences.

Primary Geolocation Methods

1. IP-Based Geolocation

IP-based geolocation relies on databases that map IP addresses to physical locations. These databases are built and maintained by specialized companies that gather data from multiple sources:

- Direct information from ISPs and RIRs
- WHOIS registration data
- Network routing information
- User-contributed location data
- Wi-Fi access point mapping

When you connect to a website, your IP address is sent to an IP-to-geolocation database that returns the approximate location data associated with that address.

2. Device-Based Geolocation

Device-based geolocation relies on GPS chips in mobile devices, Wi-Fi triangulation, and cellular network data to determine location. This method:

- Is more accurate than pure IP-based methods
- Requires explicit user permission
- Works best in densely populated areas
- Depends on the device having location services enabled

3. Combined Data Collection

Modern geolocation services often use hybrid approaches, combining multiple data sources for improved accuracy:

- IP address information
- Device GPS data (when available)
- Wi-Fi access point mapping
- Bluetooth beacons
- Cellular tower triangulation
- User-provided information

Technical Implementation

Geolocation Databases

IP geolocation databases form the backbone of the technology. These databases:

- Contain millions of IP address ranges mapped to geographical locations
- Are updated regularly to reflect changes in IP assignments
- Vary in accuracy, coverage, and update frequency
- Come in both free and commercial versions

Popular providers include MaxMind, IP2Location, and Digital Element.

Geolocation APIs

For developers, geolocation APIs provide a simple way to integrate location intelligence into applications:

```
// Example using the browser's Geolocation API
if (navigator.geolocation) {
  navigator.geolocation.getCurrentPosition(
    (position) => {
      const latitude = position.coords.latitude;
      const longitude = position.coords.longitude;
      console.log(`User location: ${latitude}, ${longitude}`);
    },
    (error) => {
      console.error('Error getting location:', error.message);
    }
  );
} else {
  console.error('Geolocation is not supported by this browser.');
}
```

Server-side APIs can also determine location from IP addresses without user permission:

```
// Example using a server-side IP geolocation API
async function getLocationFromIP(ipAddress) {
  const response = await fetch(`https://api.example.com/geoip/${ipAddress}`);
  const data = await response.json();
  return data;
}
```

Accuracy of IP Geolocation

How precise is IP geolocation? The answer depends on multiple factors:

Accuracy by Geographic Level

According to industry benchmarks from 2025:

- Country level: 98-99% accuracy
- Region/state level: 90-95% accuracy
- City level: 80-90% accuracy
- Postal/ZIP code level: 70-80% accuracy
- Specific street/building: Generally not possible with IP alone

Premium services like Digital Element's NetAcuity claim even higher accuracy rates: 99.99% at country level and 97%+ at city level globally.

Factors Affecting Accuracy

Several factors can impact geolocation accuracy:

1. IP Address Types

- **Static IPs**: More likely to have accurate location data
- **Dynamic IPs**: May have outdated location information if recently reassigned
- **Mobile IPs**: Can show the location of cellular towers rather than actual device location
- **Corporate IPs**: May show headquarters location rather than branch offices

2. Location Masking Technologies

- **VPNs**: Show the VPN server location instead of user location
- **Proxies**: Display the proxy server location
- **Tor**: Masks the original IP address through multiple relays

According to recent research, VPN usage grew by 41% between 2023 and 2025, significantly impacting geolocation accuracy for millions of users. If you're concerned about privacy, learn more about proxy servers for anonymous web browsing or how to hide your IP address.

3. Database Quality

- Update frequency
- Data sources used
- Coverage of different regions
- Verification methodologies

Business Applications of IP Geolocation

IP geolocation offers numerous benefits across industries:

Marketing and Personalization

- **Targeted advertising**: Deliver regionally relevant ads and promotions
- **Local content delivery**: Show content in the right language and cultural context
- **Currency and pricing adaptation**: Display prices in local currency
- **A/B testing by region**: Test different strategies in different markets

According to a 2024 study by Marketing Insider, location-based personalization increased conversion rates by 32% and customer satisfaction by 27%.

Fraud Detection and Security

- **Suspicious login detection**: Flag logins from unusual locations
- **Transaction verification**: Verify that payment locations match customer profiles
- **Bot and attack mitigation**: Identify and block traffic from high-risk regions
- **VPN/proxy detection**: Identify users attempting to mask their true location

Content Licensing and Distribution

- **Digital rights management**: Enforce regional licensing agreements
- **Content geo-restrictions**: Limit access to region-specific content
- **Localized content delivery**: Serve region-appropriate versions of websites

Compliance and Regulation

- **Data sovereignty**: Ensure data is processed according to local laws
- **GDPR and privacy regulations**: Apply appropriate privacy controls by region
- **Age verification**: Enforce regional age restrictions
- **Gambling and restricted products**: Comply with regional restrictions

Analytics and Business Intelligence

- **Traffic analysis**: Understand where visitors come from
- **Market penetration**: Identify strong and weak regional markets
- **Competitive analysis**: Compare regional performance against competitors

For companies involved in data collection, check our guide on web scraping best practices for ethically gathering and using location-based data.

Real-World Case Study: E-Commerce Optimization

In 2023, an international e-commerce retailer implemented advanced IP geolocation to optimize their customer experience. The results were striking:

- 43% reduction in cart abandonment by automatically showing correct shipping costs and delivery times based on location
- 28% increase in conversion rates through localized promotions and pricing
- 67% reduction in fraudulent transactions by implementing location-based verification
- 22% improvement in customer satisfaction scores from better personalization

According to their CTO: "Implementing advanced geolocation was one of our highest ROI investments of the year. Beyond the direct revenue impact, it gave us insights that changed our entire regional strategy."

Privacy Implications and Ethical Considerations

IP geolocation raises important privacy questions that businesses must consider:

User Consent and Transparency

While IP-based geolocation doesn't legally require consent in most jurisdictions (unlike GPS tracking), best practices and evolving regulations increasingly demand transparency about:

- What location data is collected
- How it's used
- How long it's retained
- Who it's shared with

Regulatory Landscape

Geolocation data is increasingly regulated under frameworks like:

- **GDPR in Europe**: Considers location data as personal information requiring protection
- **CCPA/CPRA in California**: Gives users rights regarding their location data
- **LGPD in Brazil**: Requires consent for most location tracking
- **The American Data Privacy and Protection Act**: Proposed legislation that would create federal standards for location privacy

The Balance: Privacy vs. Functionality

The growing tension between useful personalization and privacy is creating new approaches:

- **Privacy-preserving geolocation**: Technologies that provide approximate location without precise tracking
- **Federated location processing**: Processing location data on-device rather than in the cloud
- **Progressive disclosure**: Starting with minimal location data and requesting more specific information only when needed

Implementing IP Geolocation: Best Practices

For businesses looking to implement geolocation, following these best practices can maximize benefits while minimizing risks:

Technical Implementation

1. **Choose the right provider**: Select a geolocation database or API based on your accuracy needs, budget, and regions of operation
2. **Implement caching**: Cache location results to reduce API calls and improve performance
3. **Use fallback methods**: Have alternatives when primary geolocation methods fail
4. **Verify critical locations**: For security or compliance-critical applications, use multiple verification methods

Ethical Implementation

1. **Be transparent**: Clearly disclose your use of geolocation in privacy policies
2. **Provide value**: Ensure your use of location data benefits users, not just your business
3. **Minimize data**: Collect only the level of location detail you actually need

4. **Respect preferences**: Honor Do Not Track and similar opt-out signals
5. **Secure data**: Treat location data as sensitive and protect it accordingly

The Future of IP Geolocation

The geolocation landscape is evolving rapidly, with several emerging trends:

Technological Advancements

- **Machine learning enhancements**: ML algorithms that improve accuracy by analyzing patterns in network traffic
- **IPv6 challenges and opportunities**: The massive increase in available addresses changes how geolocation works
- **IoT device geolocation**: Specialized methods for locating the growing number of connected devices
- **Advanced identification methods**: Including techniques like browser fingerprint detection that complement traditional IP-based location

Privacy Innovations

- **Differential privacy**: Adding calibrated noise to location data to protect individual privacy while preserving aggregate insights
- **Zero-knowledge proofs**: Cryptographic methods that verify location claims without revealing exact coordinates
- **User-controlled location sharing**: Giving users granular control over what location data they share

Market Evolution

According to a 2025 Markets and Markets report, the geolocation market is projected to grow from $15.7 billion in 2024 to $25.9 billion by 2028, driven by:

- Integration with AI and big data analytics
- Growing demand for location-based marketing
- Expansion into emerging markets
- New applications in autonomous vehicles and smart cities

Technical Community Views: The Reality of IP Geolocation

Real-world experiences shared by engineers reveal significant discrepancies between the theoretical capabilities of IP geolocation and its practical implementation. Network professionals across online forums consistently emphasize that IP geolocation is fundamentally imprecise—more educated guesswork than exact science. Many experienced network administrators point out that while regional accuracy is achievable, precise location data often falls short of vendor claims.

Technical discussions highlight how IP addresses follow network topology rather than geographical boundaries. As one senior network engineer explains, IP blocks are allocated to Regional Internet Registries (RIRs) like ARIN, RIPE, and APNIC, providing some regional context, but this doesn't guarantee location accuracy. Several professionals note that even when registration data includes location information, this often points to corporate headquarters rather than where the infrastructure actually operates. One network administrator mentioned their company headquarters is in Virginia while their /24 block is advertised from New York, illustrating this disconnect.

Engineers with hands-on experience share particularly troubling insights about edge cases. Multiple IT professionals report significant location mismatches—one engineer in Virginia consistently appears in Utah according to major geolocation providers, while others report similar discrepancies. The problem compounds with anycast IP addresses used by CDNs like Fastly, where a single IP might be served from hundreds of data centers worldwide. Network teams managing their own IP space emphasize the tedious process of manually submitting correction tickets to each geolocation service, with one noting that "Microsoft's database is the hardest to correct."

The development community has been actively discussing emerging standards that might improve the situation. Some engineers highlight RFC 8805/9092, which enables IP block owners to self-publish location data through a standardized geofeed format. However, adoption remains extremely limited—one contributor who analyzed implementation in January found only about 500 feeds covering roughly 6 million IPs, representing just 0.2% of announced IP addresses. Despite this slow progress, ISP engineers confirm that when properly implemented, these feeds can systematically update geolocation services—though update frequencies vary from daily to monthly depending on the service.

While the technical consensus acknowledges geolocation's limitations, practitioners also recognize its practical utility within appropriate constraints. Network professionals generally agree that country-level filtering is reasonably reliable, making it suitable for compliance and basic content localization. However, they strongly caution against depending on IP geolocation for precise targeting or critical security decisions. As one experienced engineer summarized: "Don't depend on geolocation information unless you have to or can block at very high levels and are prepared to deal with the inevitable false positives."

Conclusion

IP geolocation has evolved from a simple mapping of IP addresses to a sophisticated technology with profound implications for business, privacy, and the online experience. As we move forward, the balance between personalization and privacy will continue to shape how this technology develops.

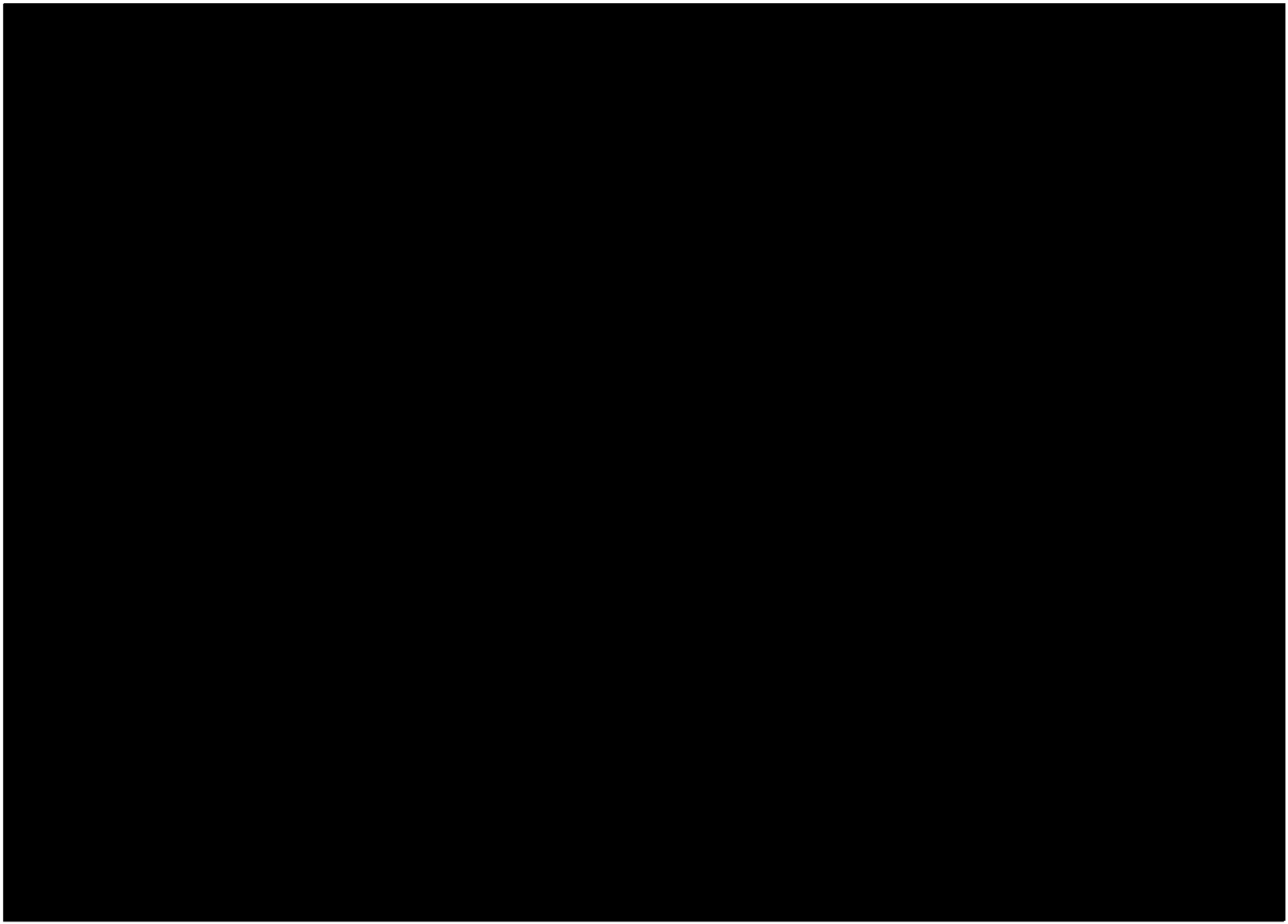
The most successful implementations will be those that provide genuine value to users while respecting their privacy preferences and maintaining transparent practices. By understanding both the technical capabilities and ethical considerations of geolocation, businesses can harness its power responsibly and effectively.

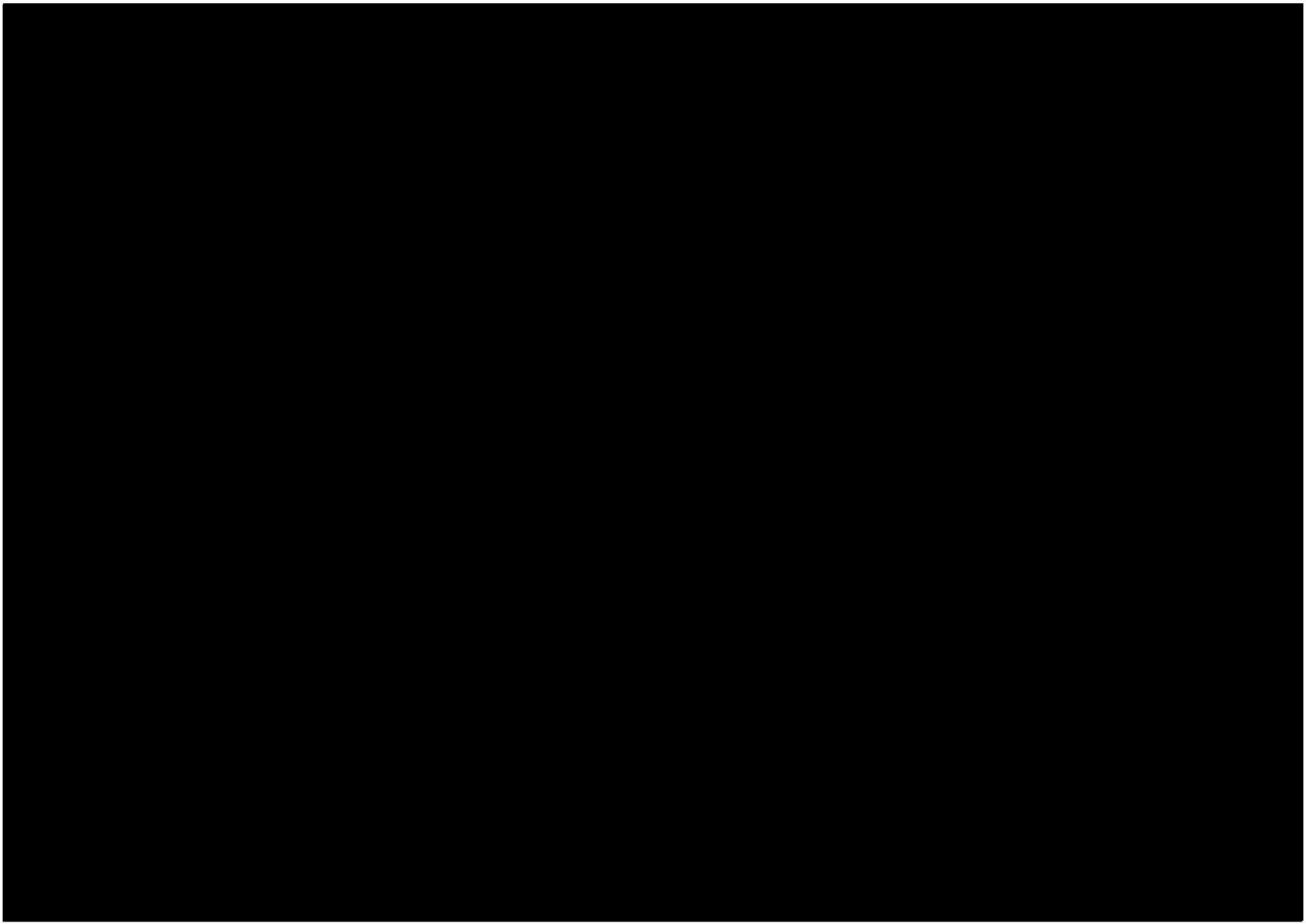
Whether you're a developer looking to implement geolocation features, a marketer seeking to improve targeting, or a business leader making decisions about customer data, staying informed about this rapidly evolving technology will be crucial in the years ahead.

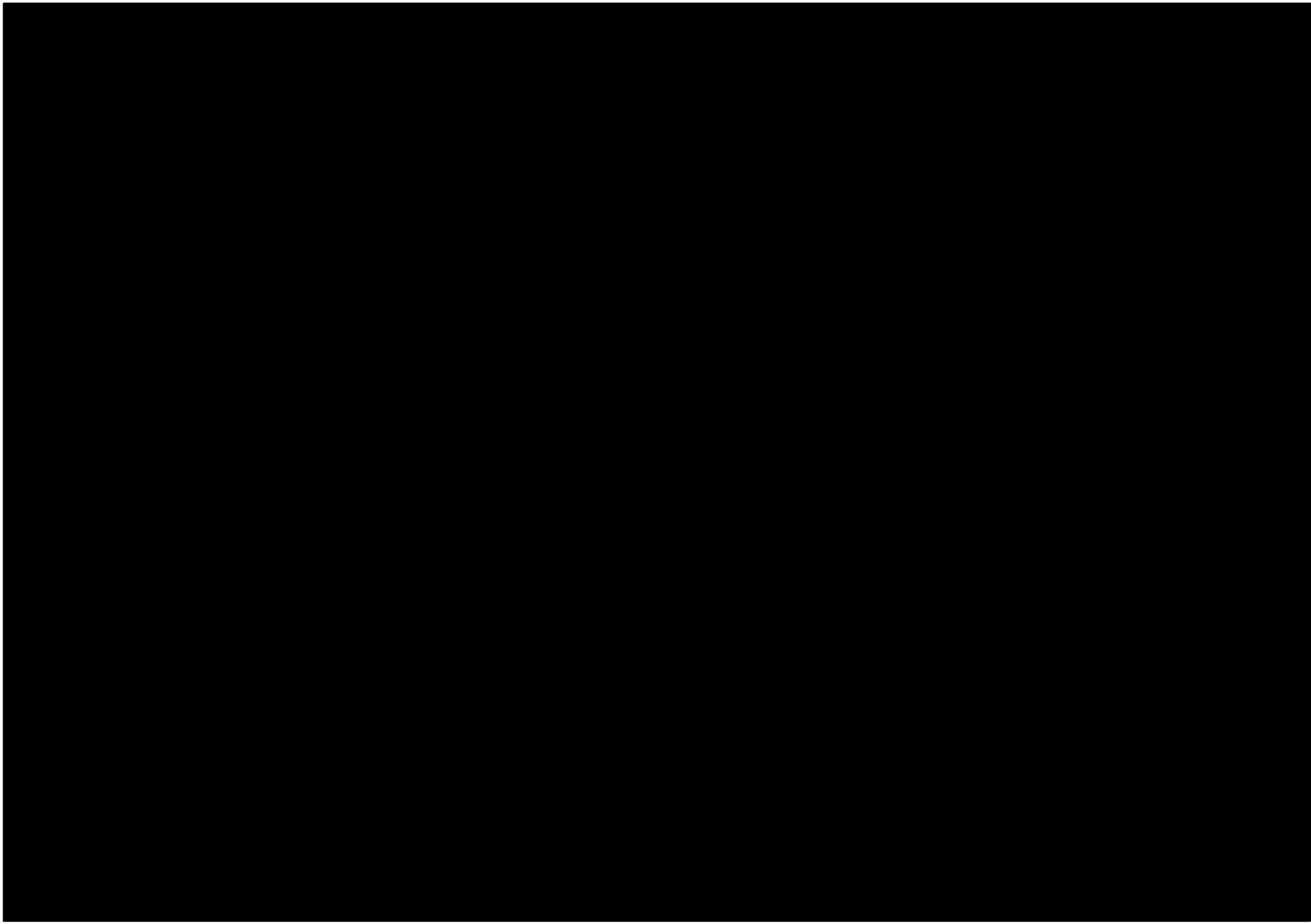
James Sanders

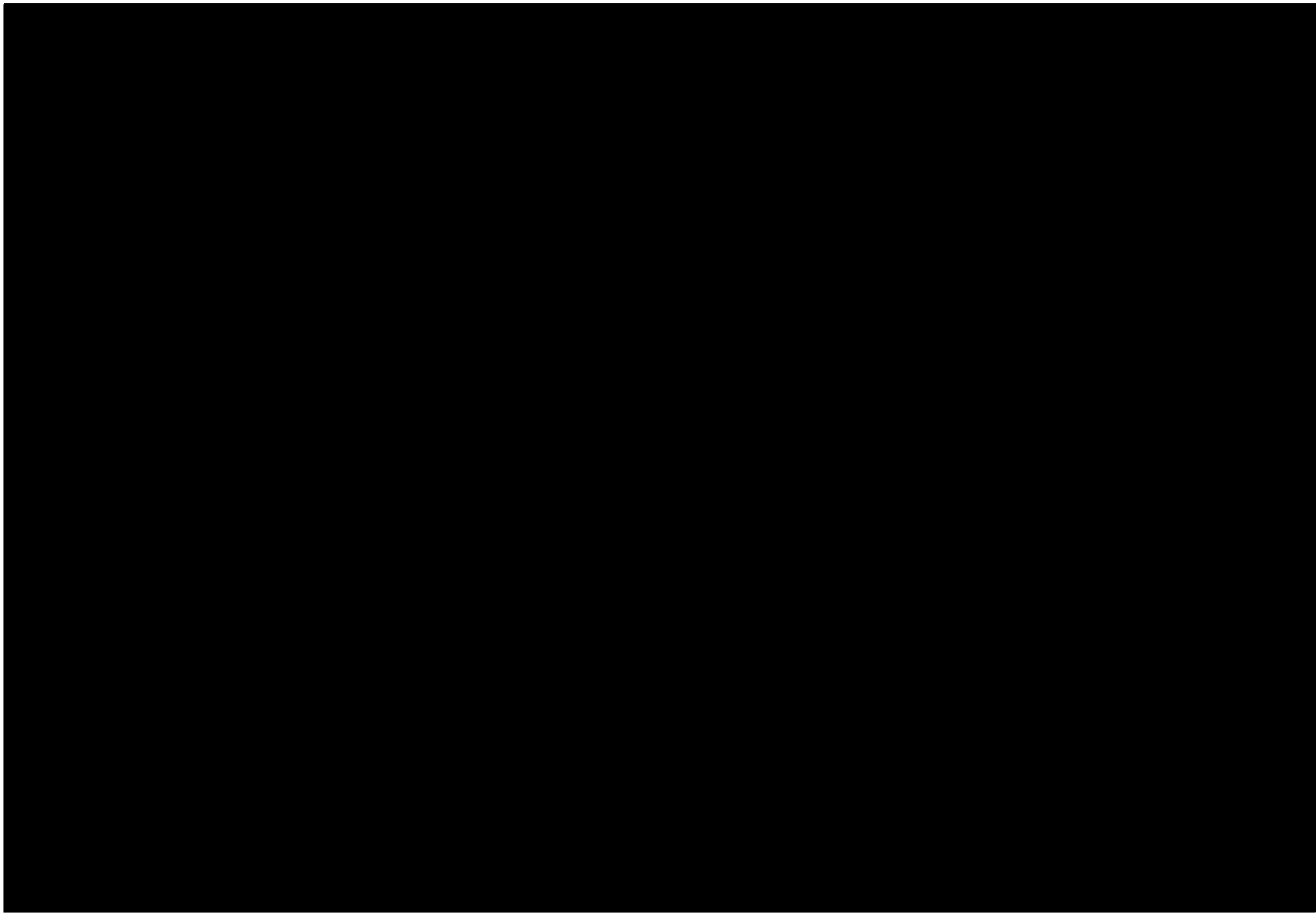
James joined litport.net since very early days of our business. He is an automation magician helping our customers to choose the best proxy option for their software. James's goal is to share his knowledge and get your business top performance.

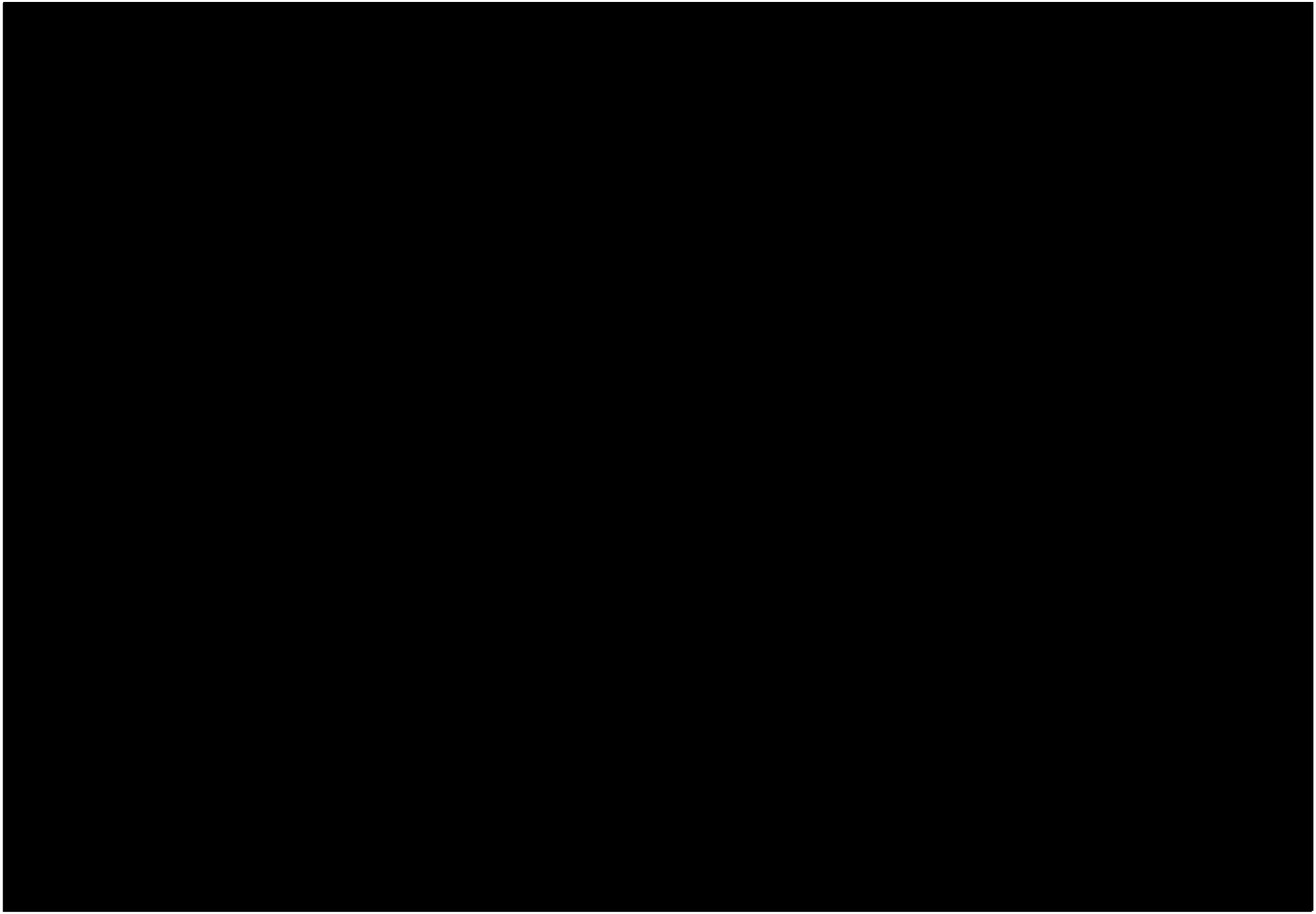
EXHIBIT D

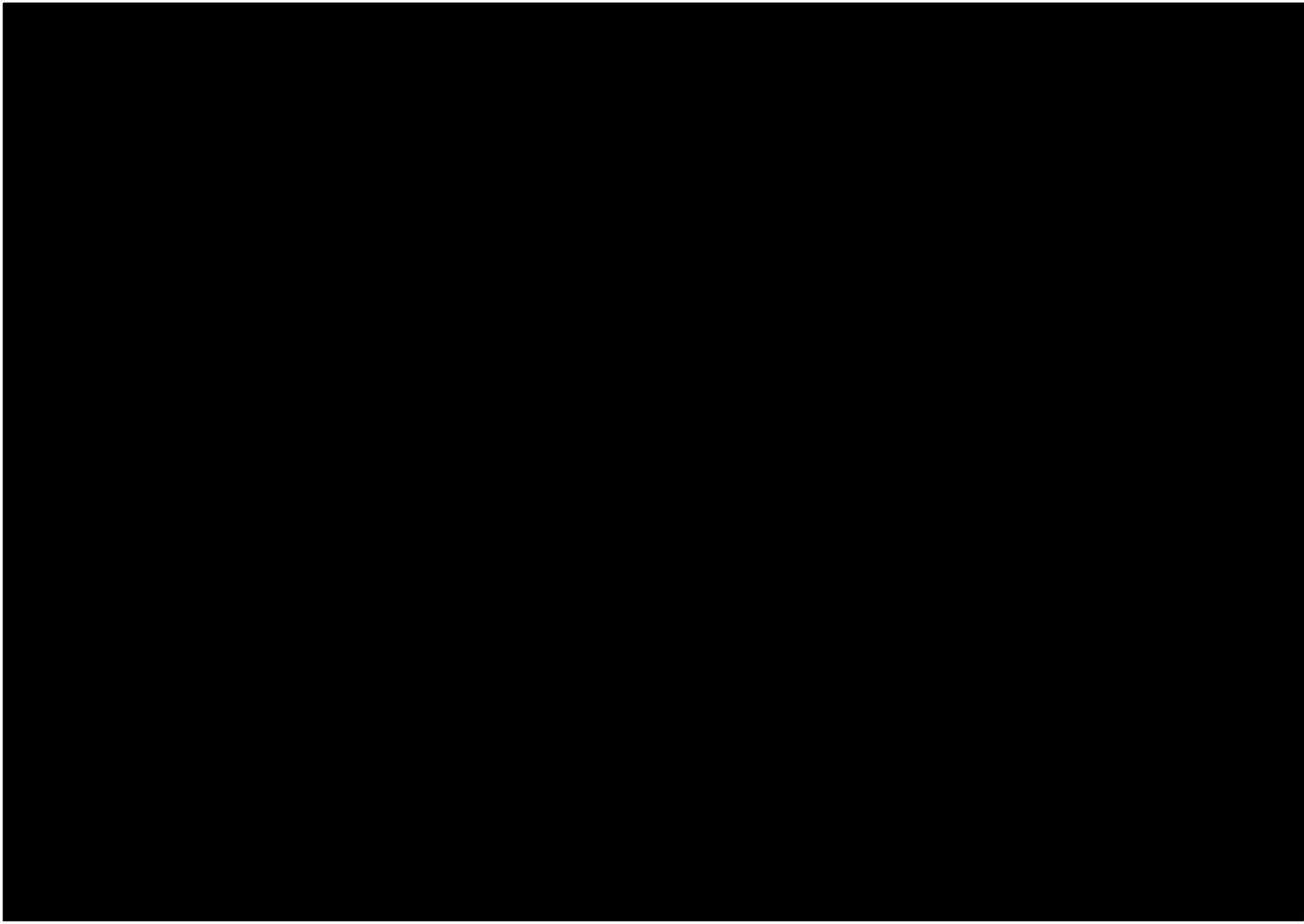


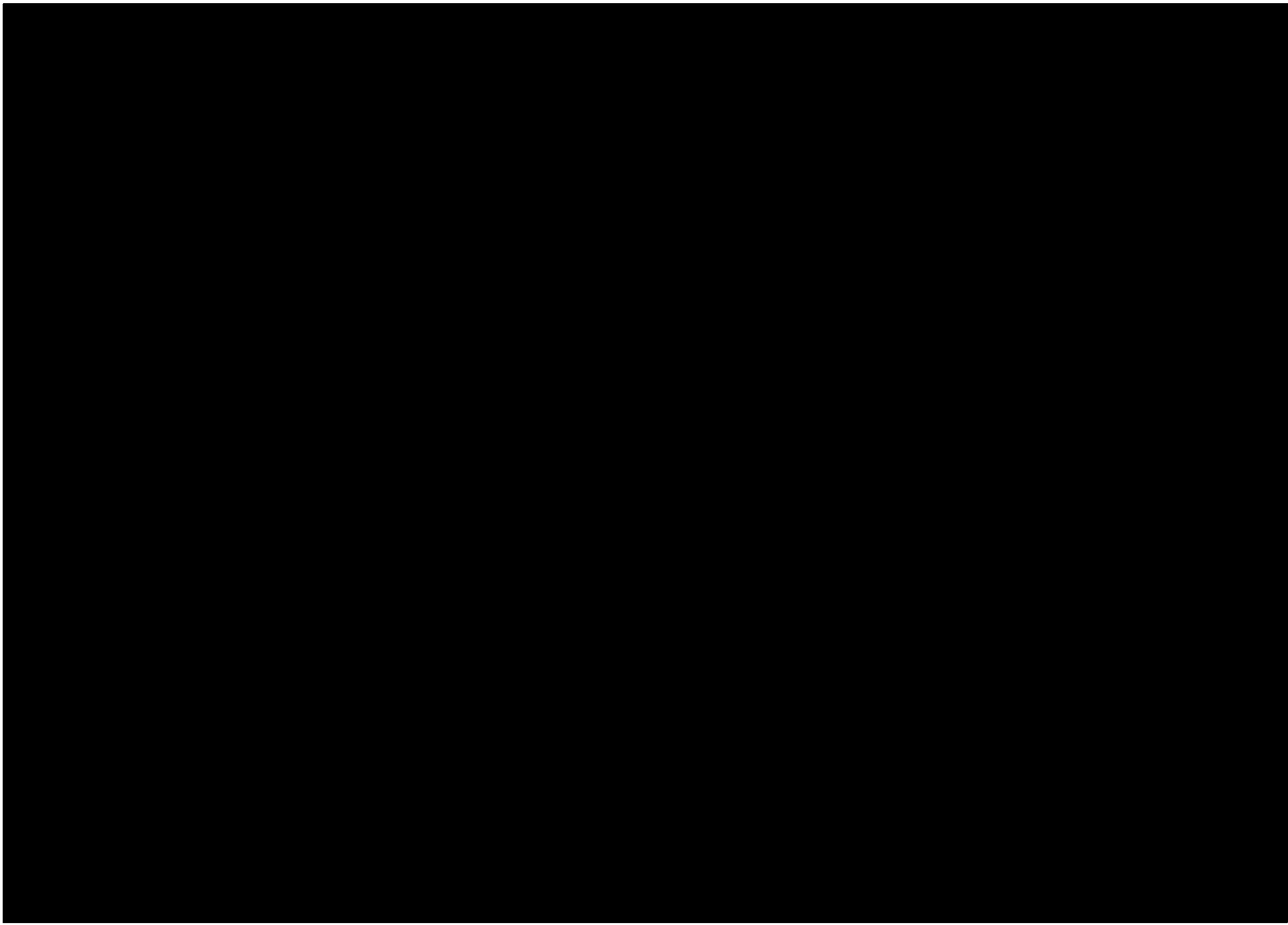


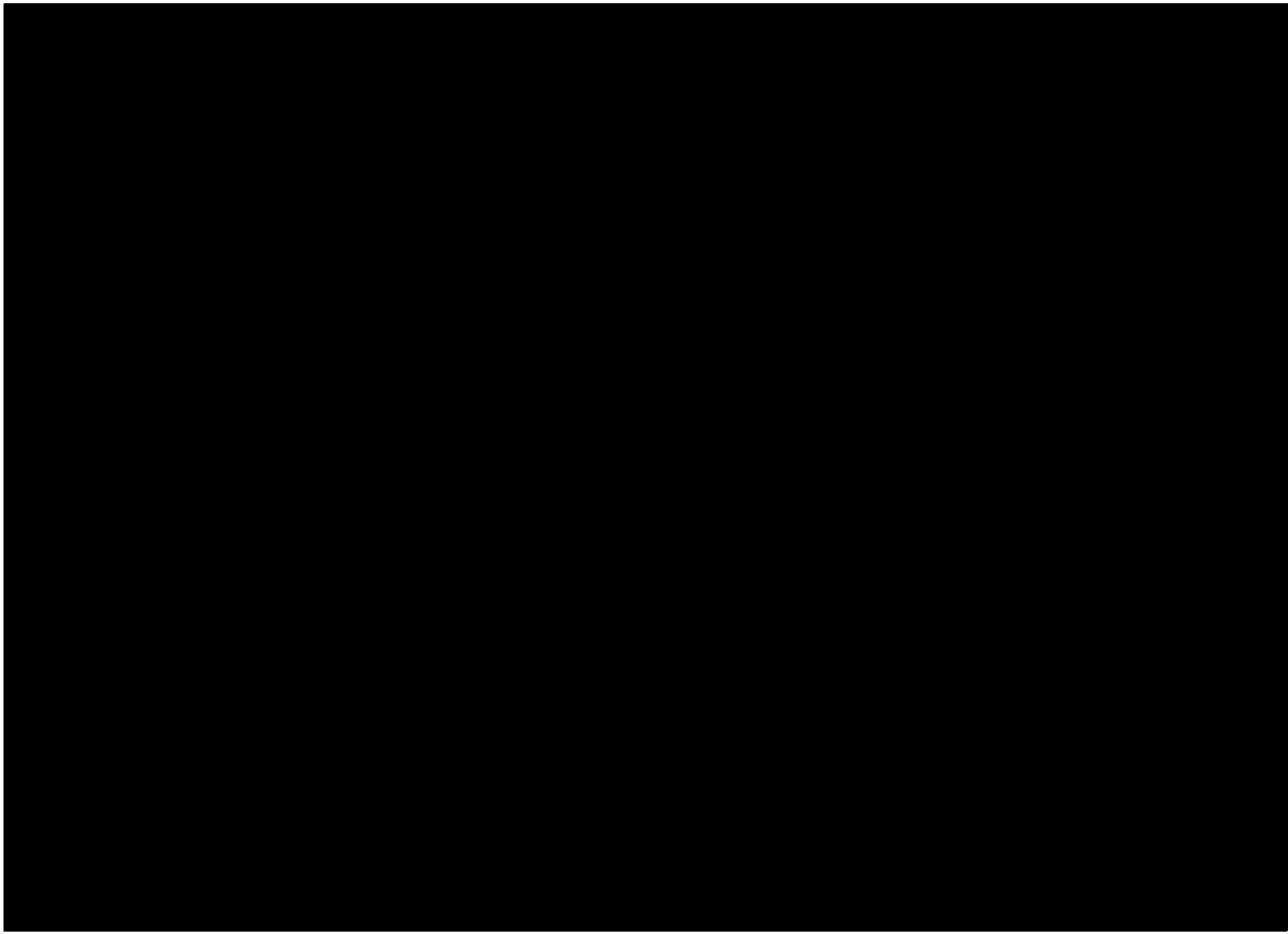


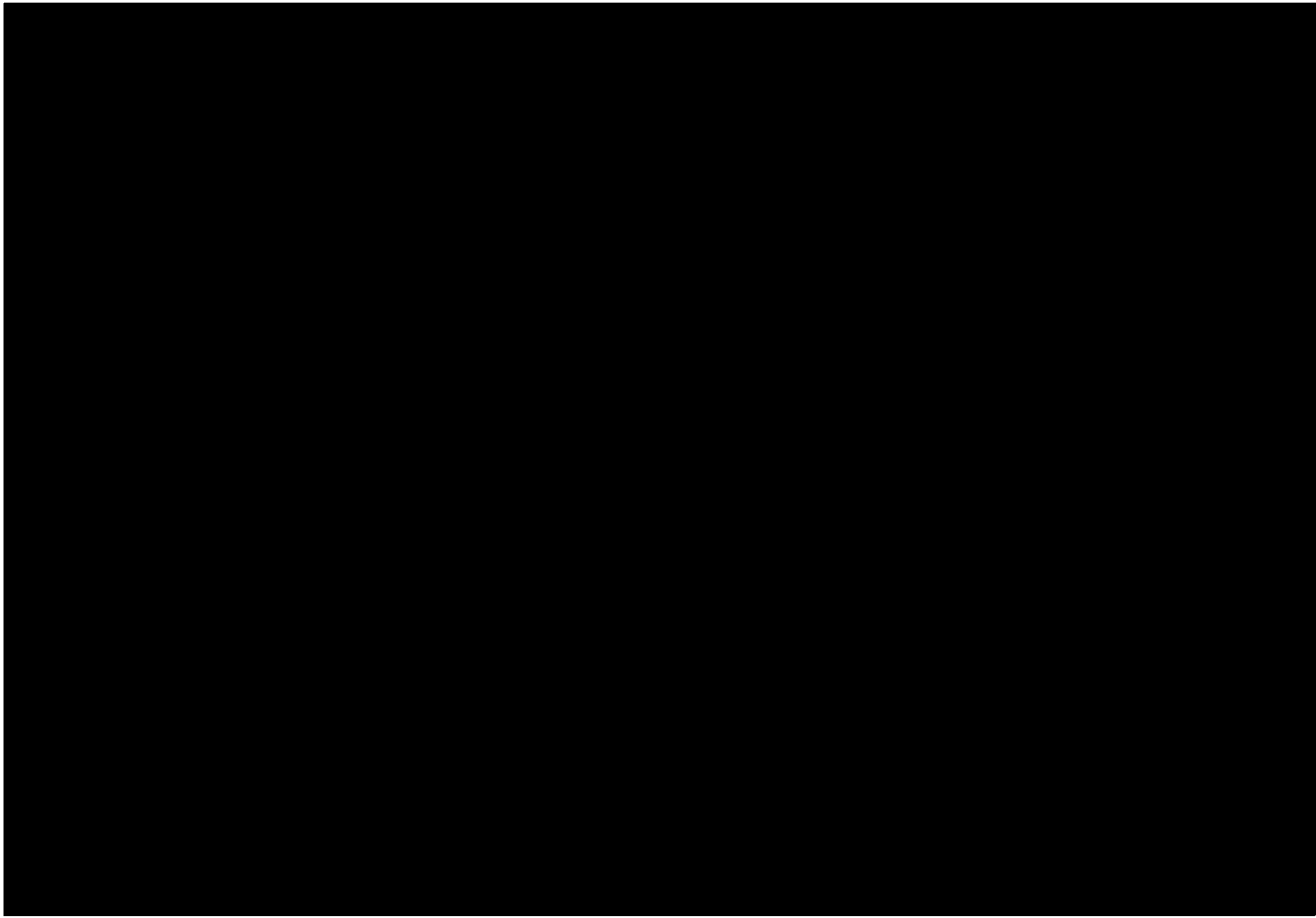


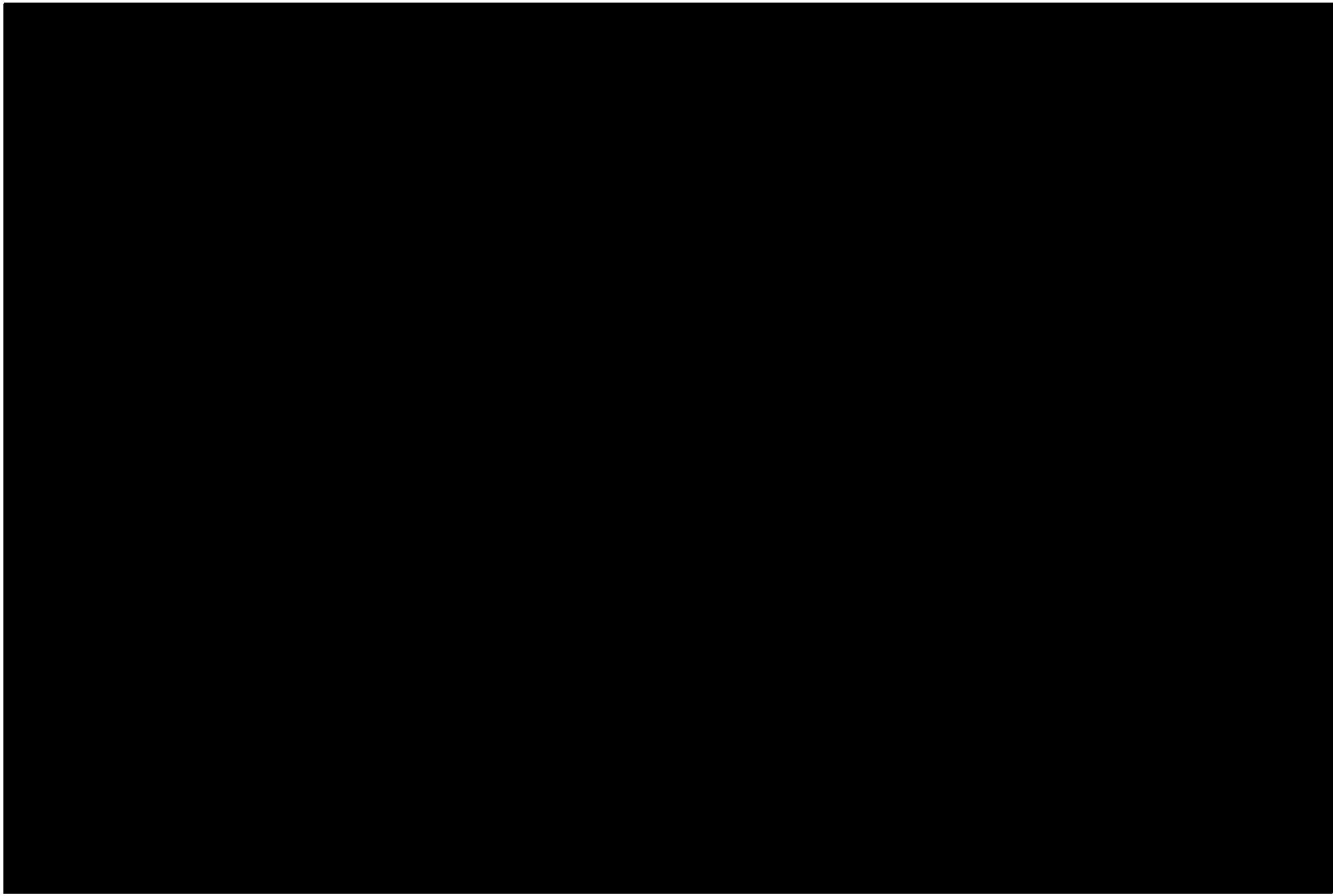


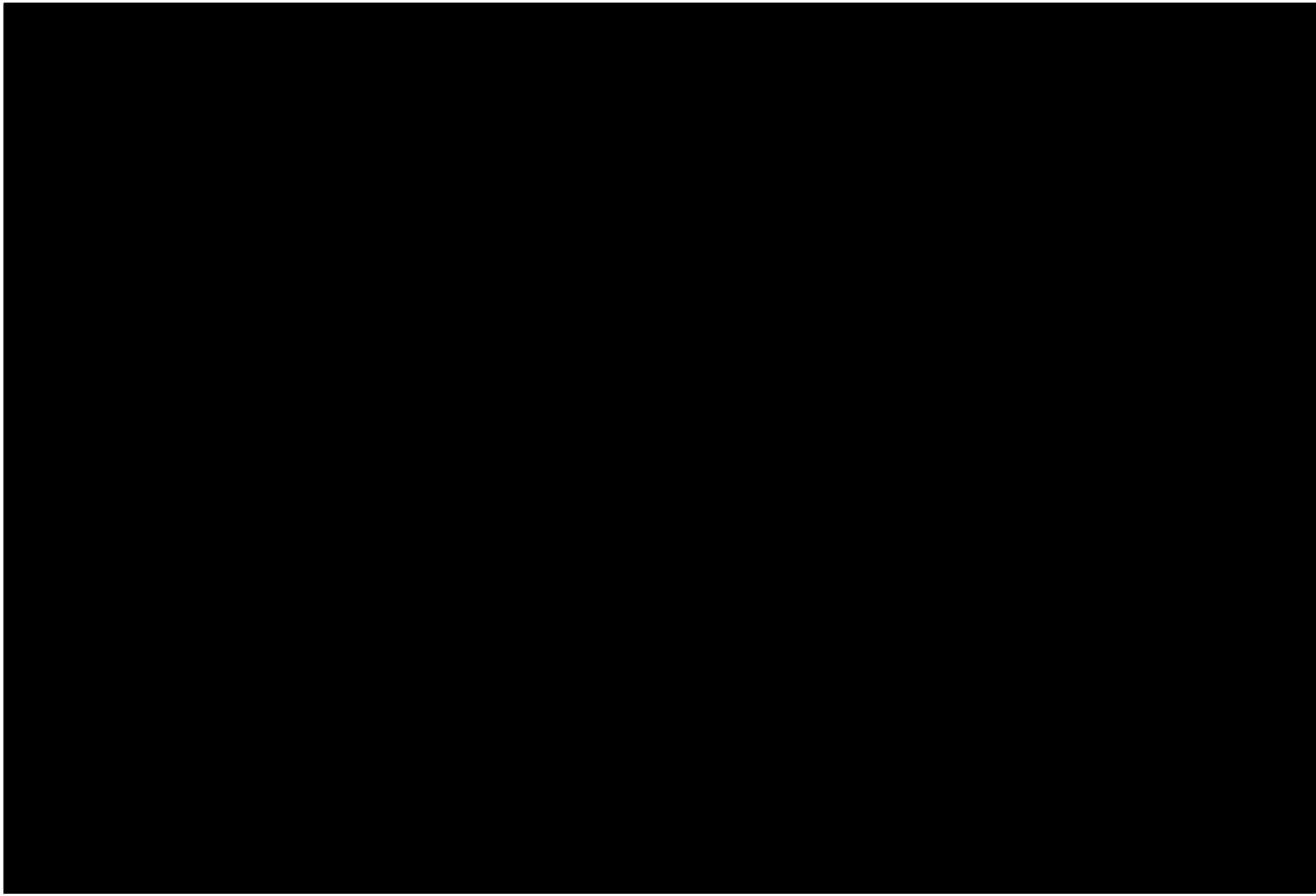


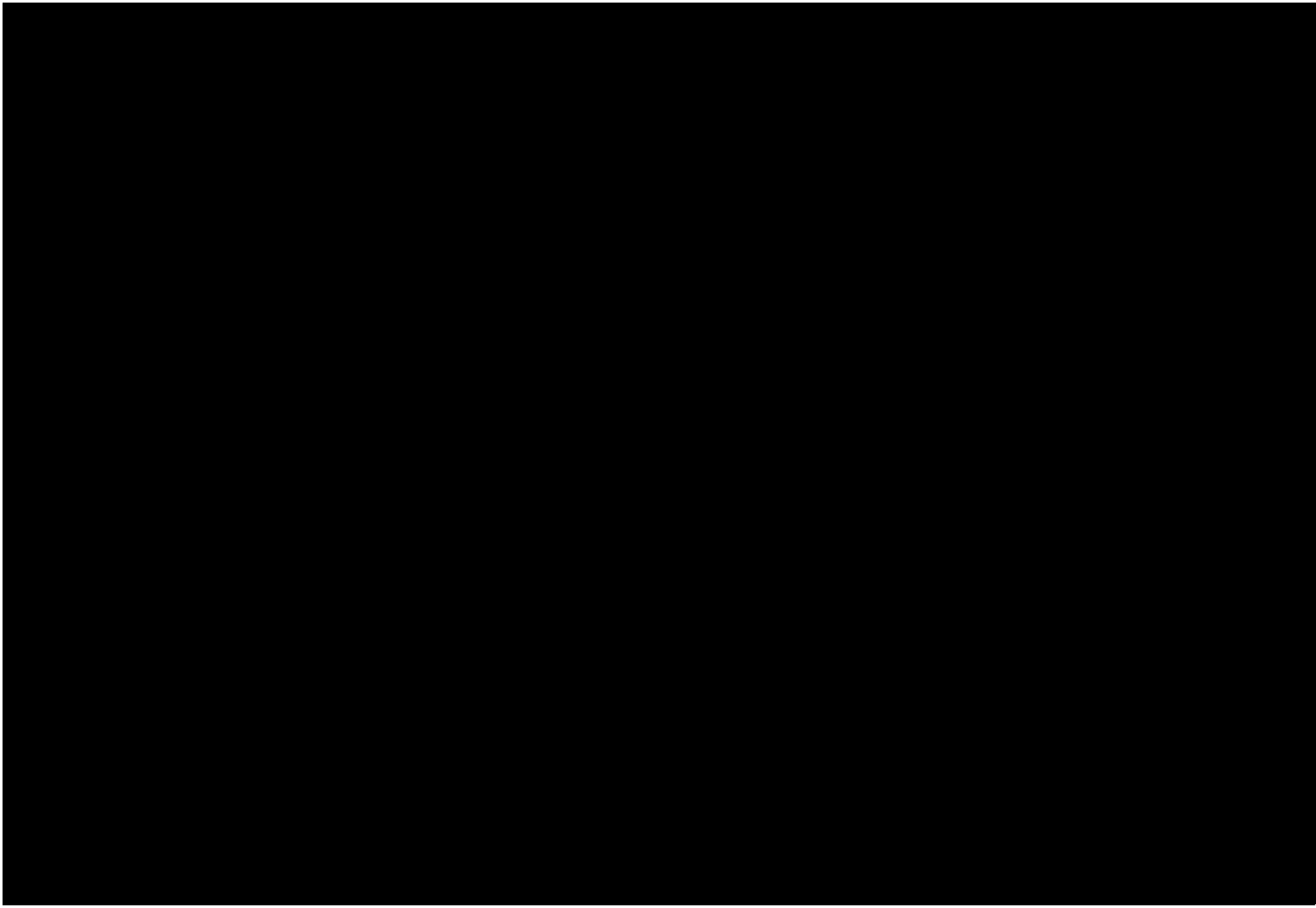


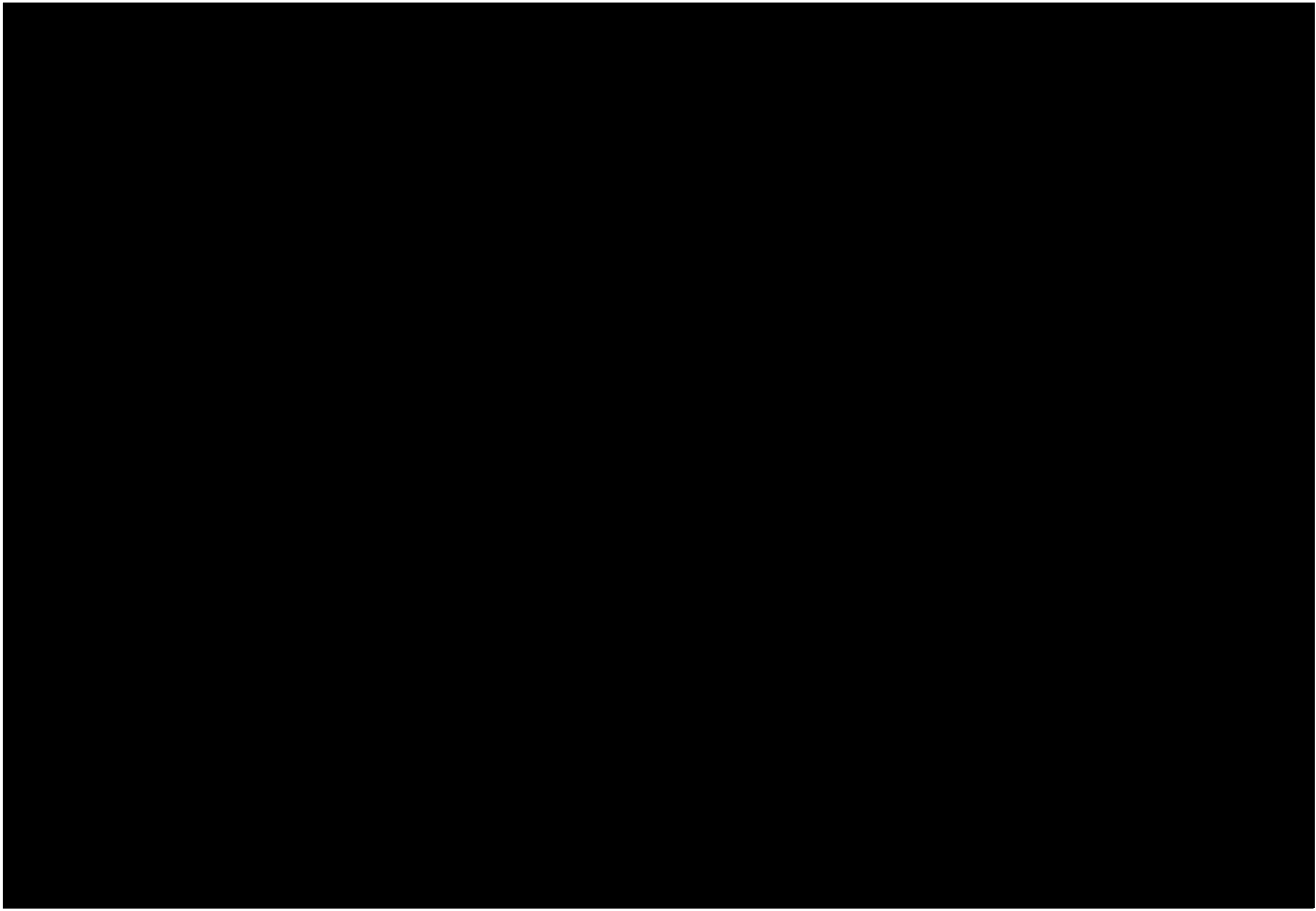


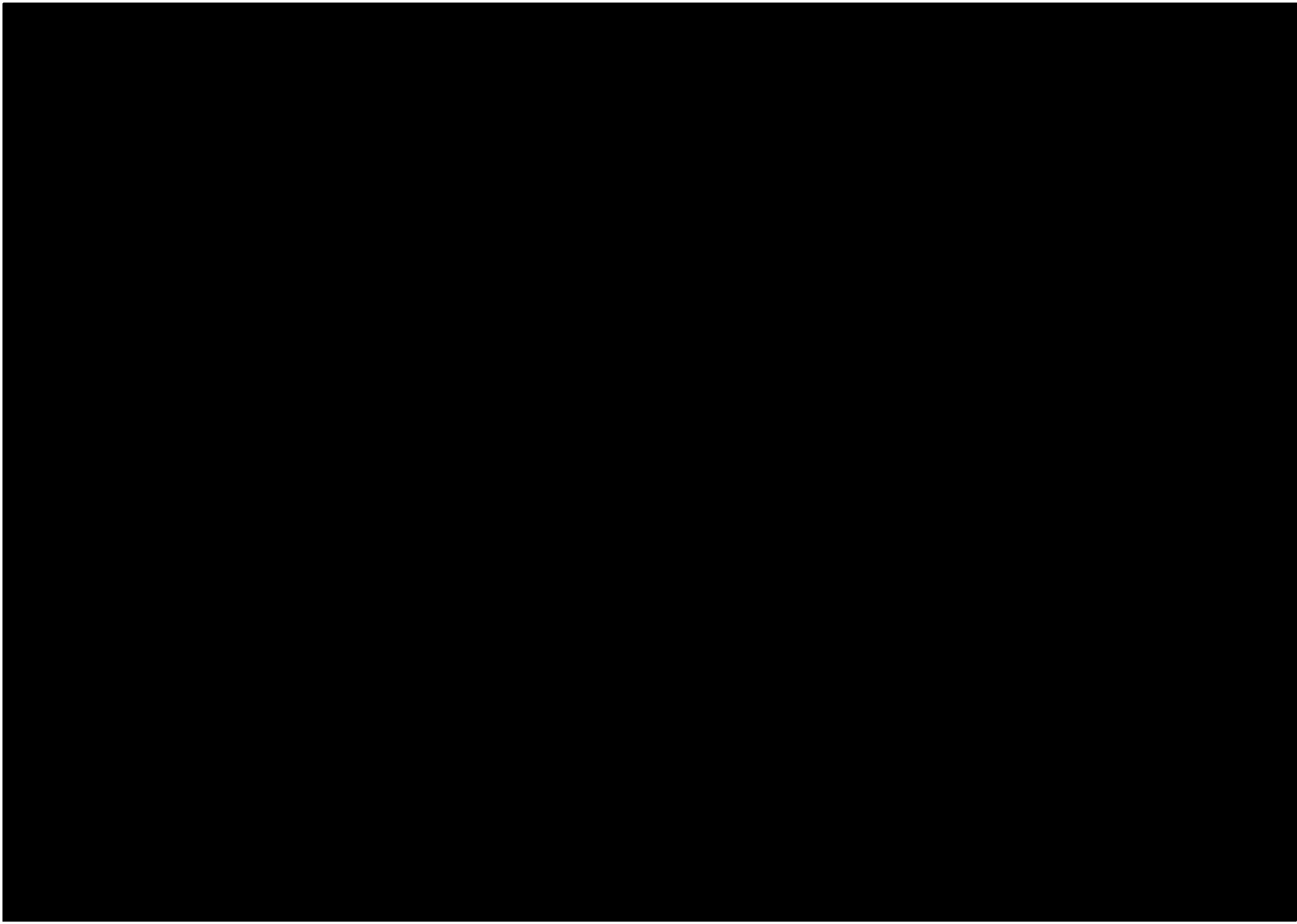












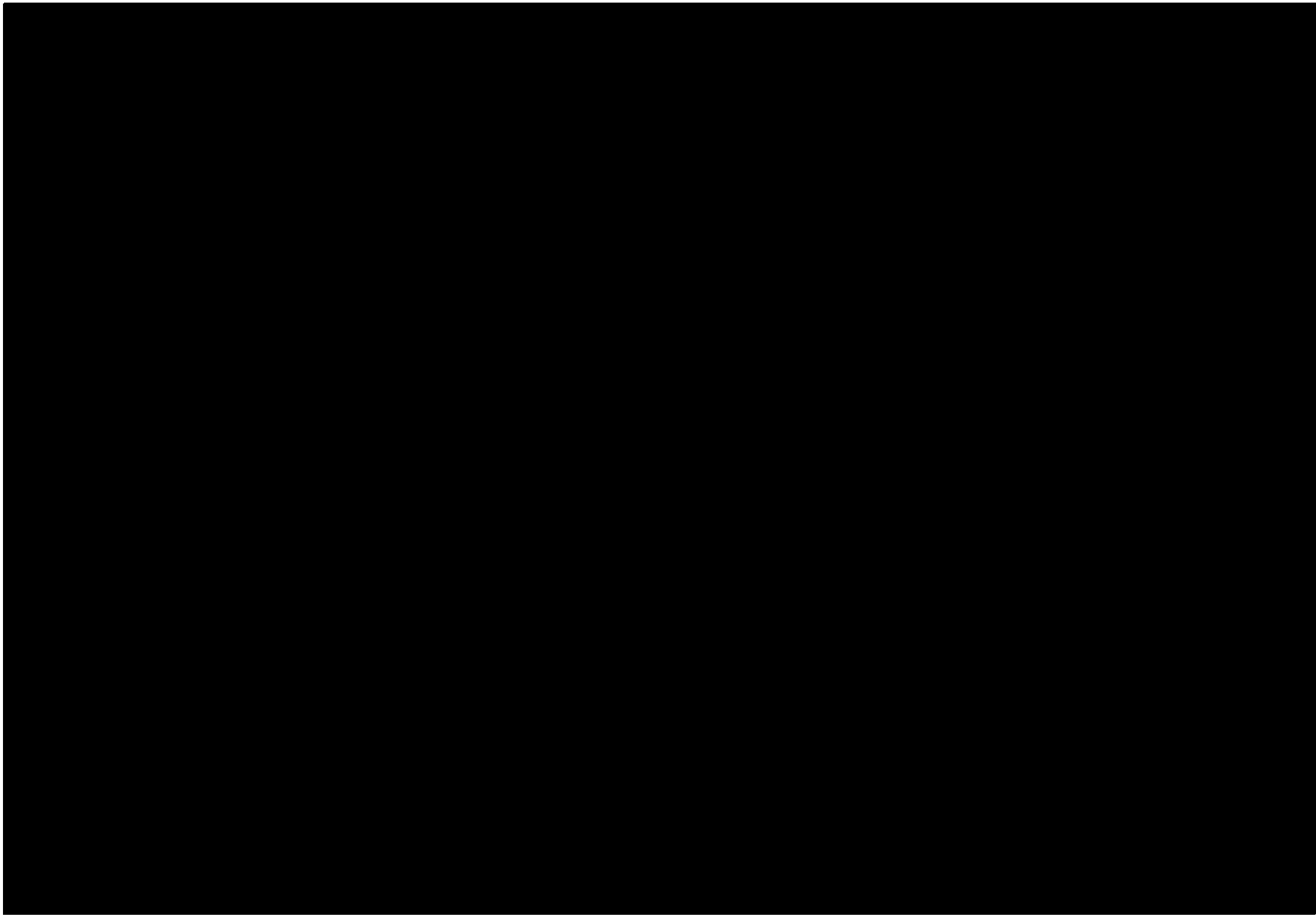
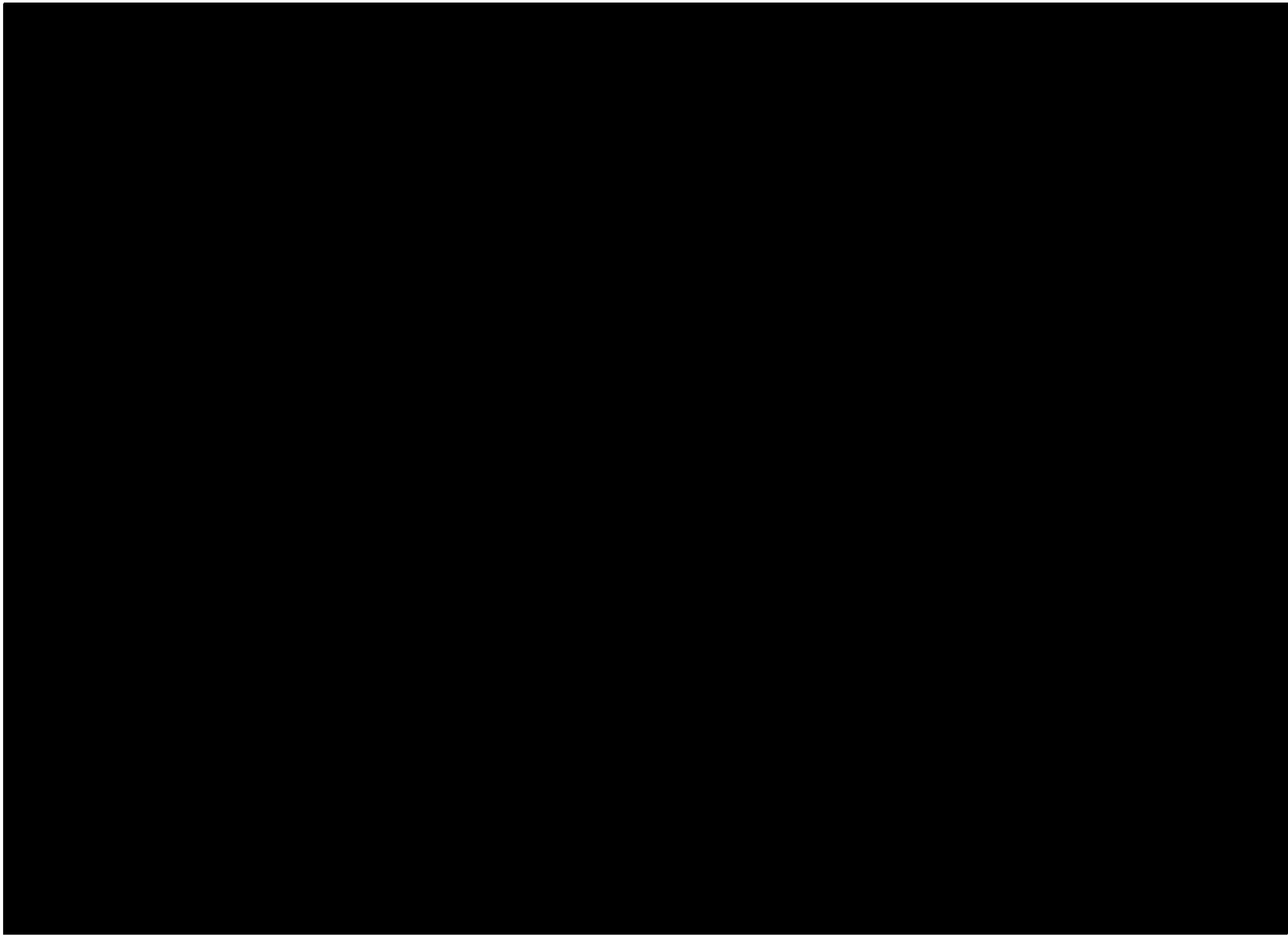
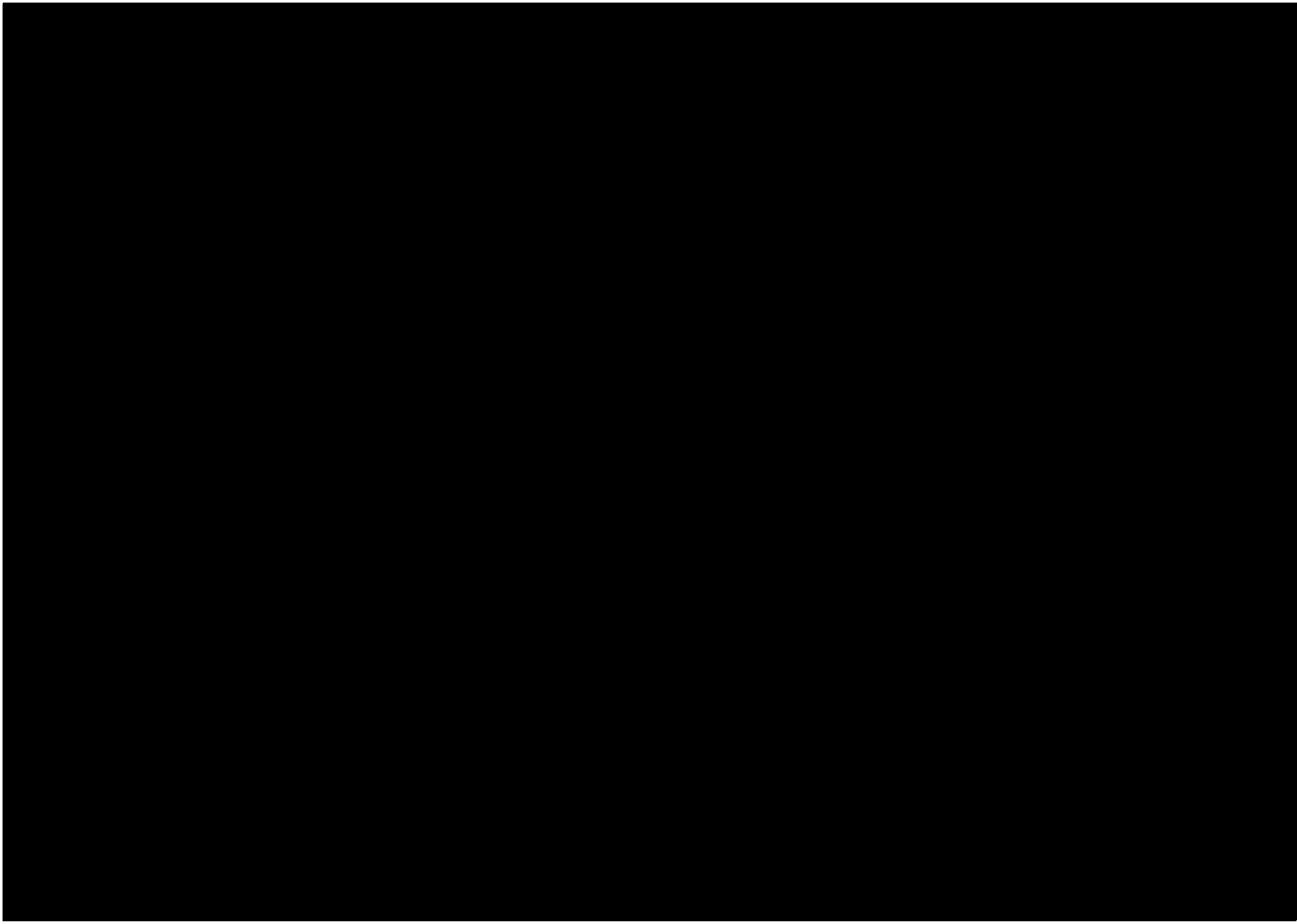
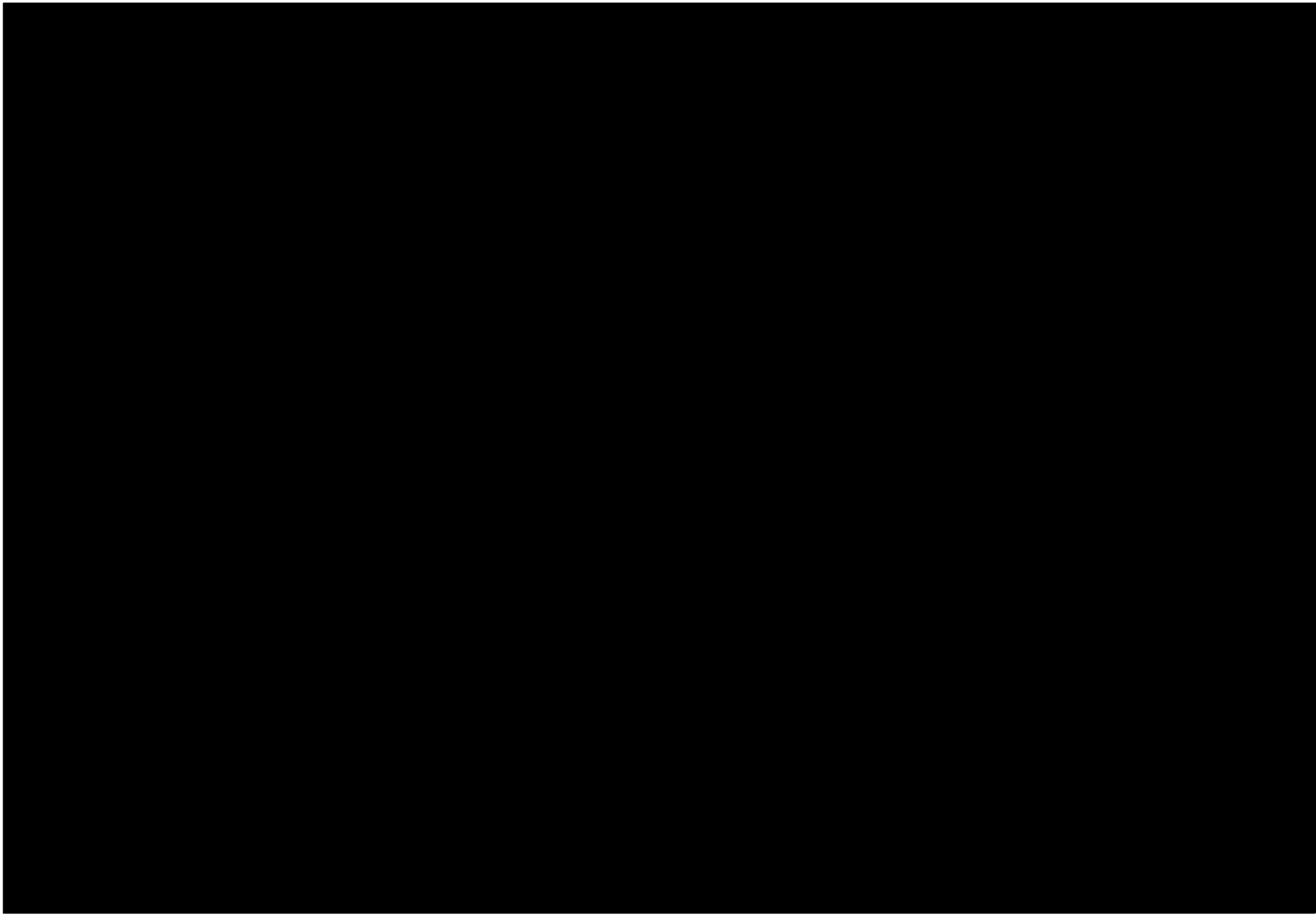
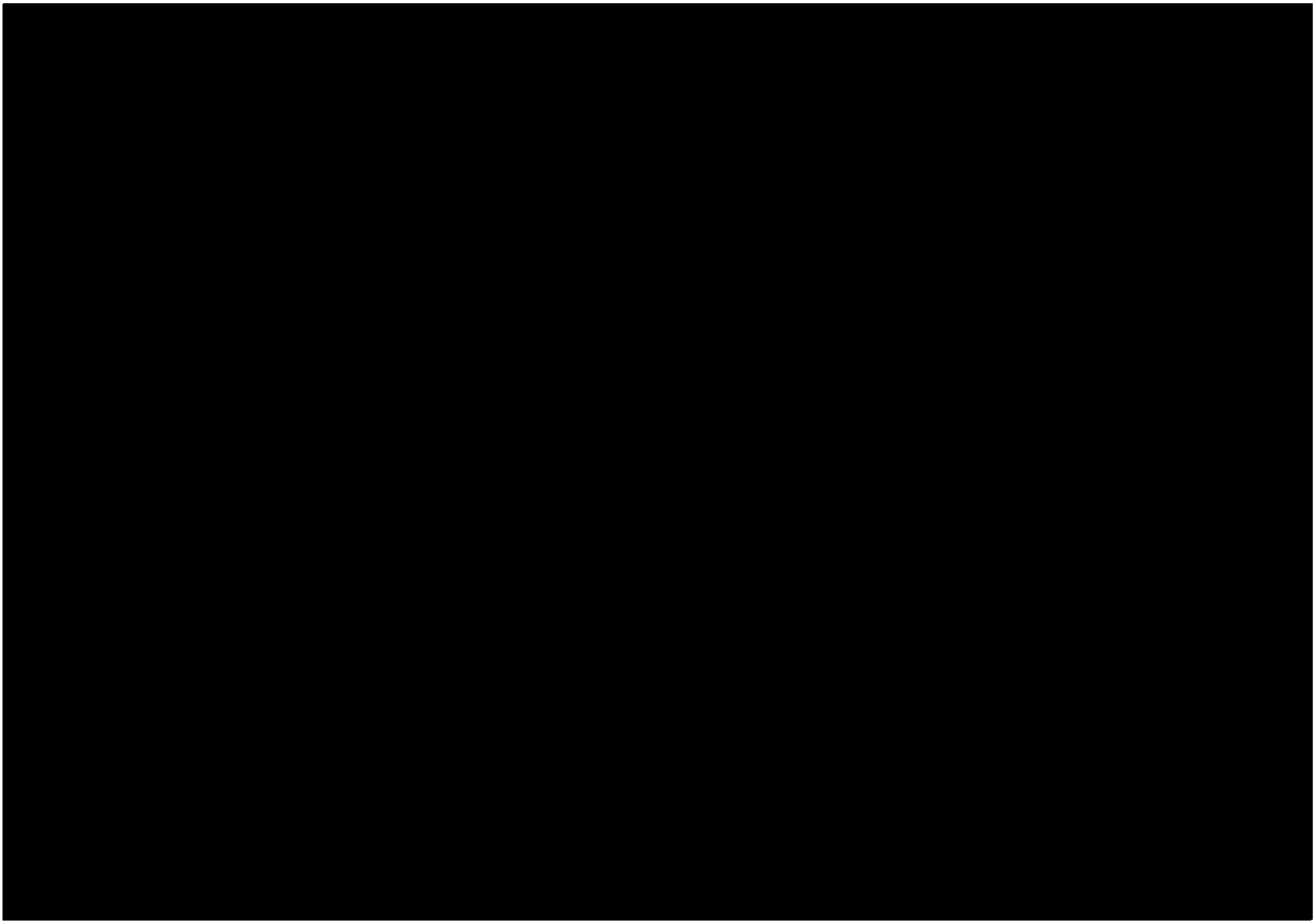


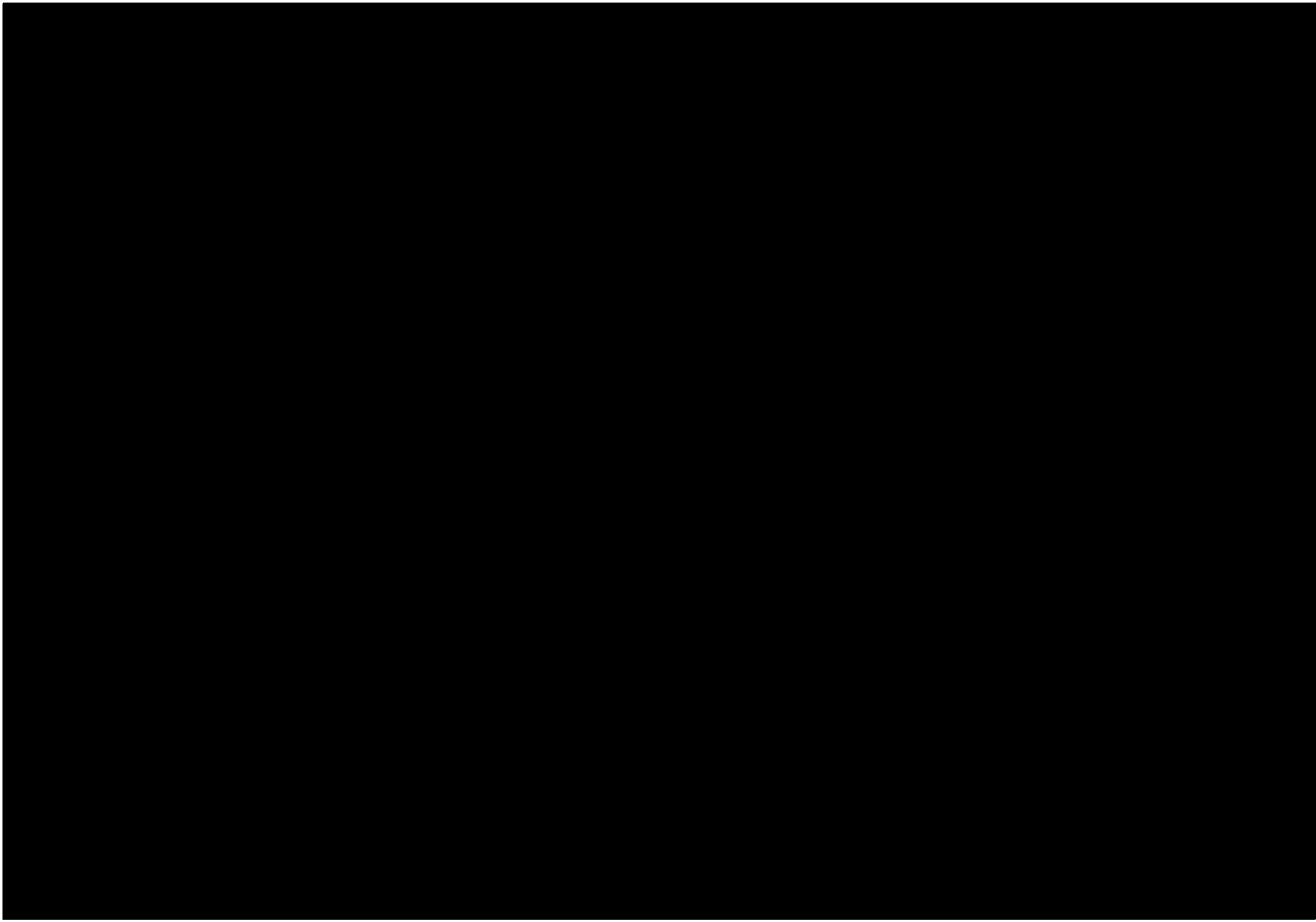
EXHIBIT E

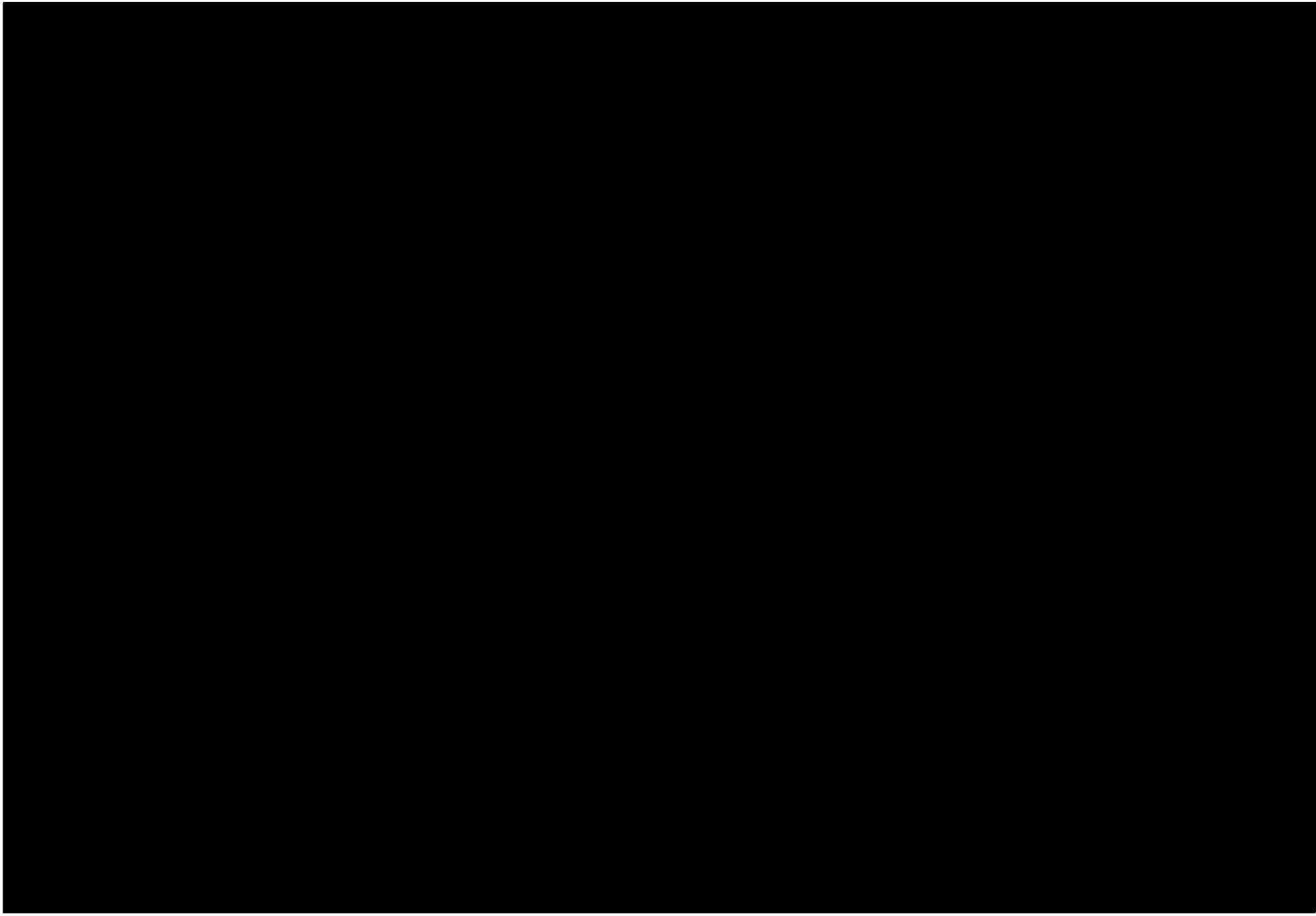


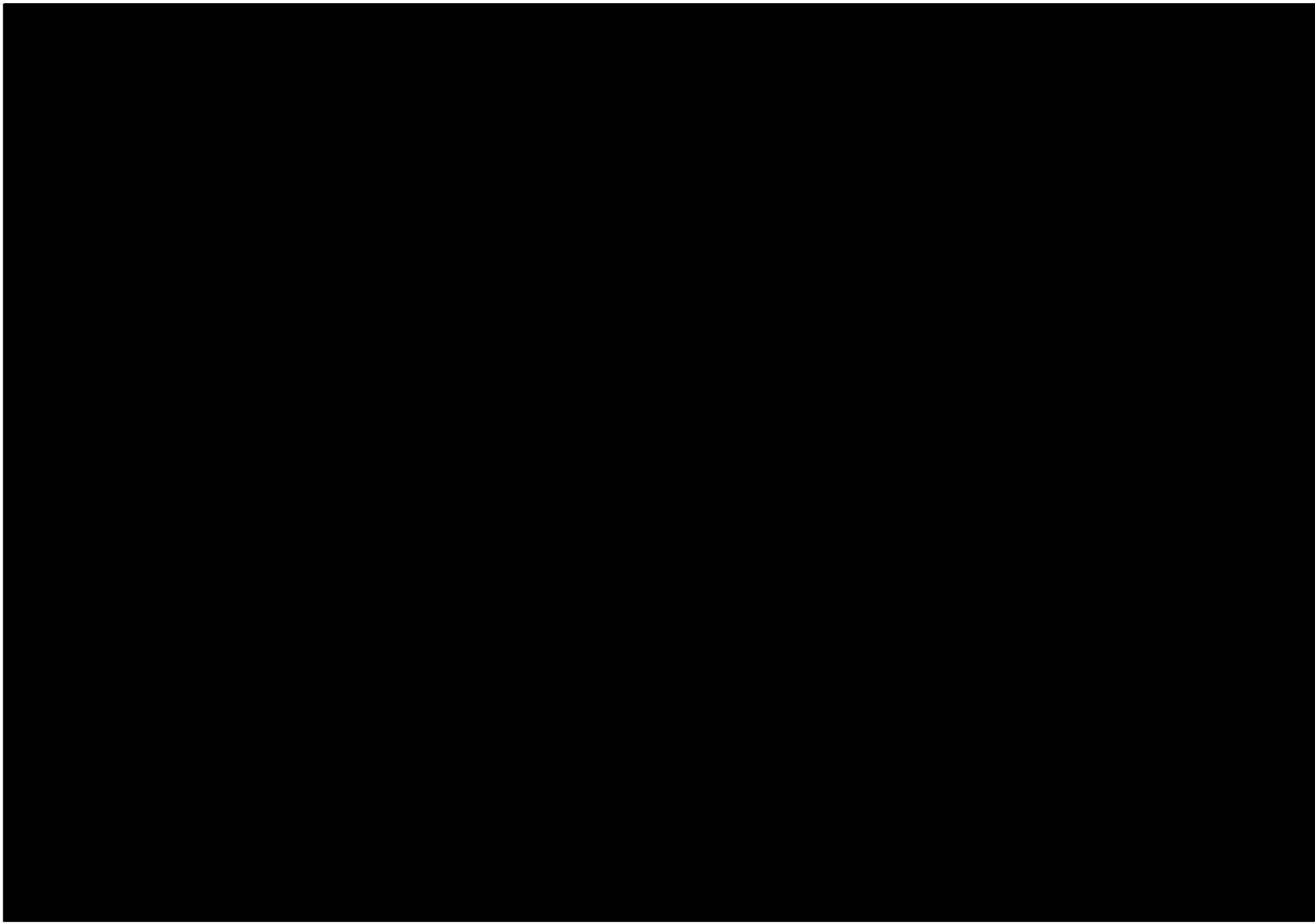


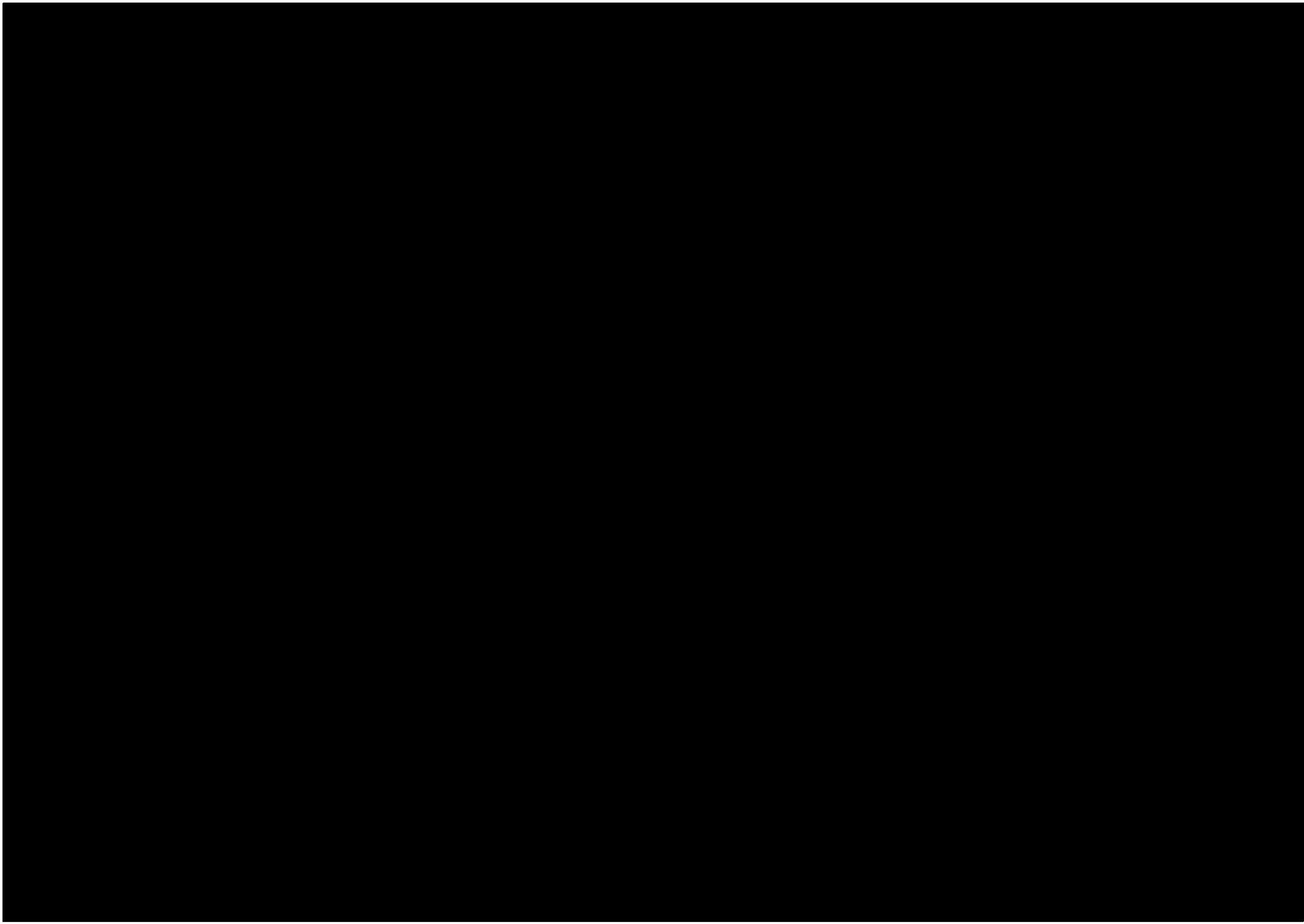


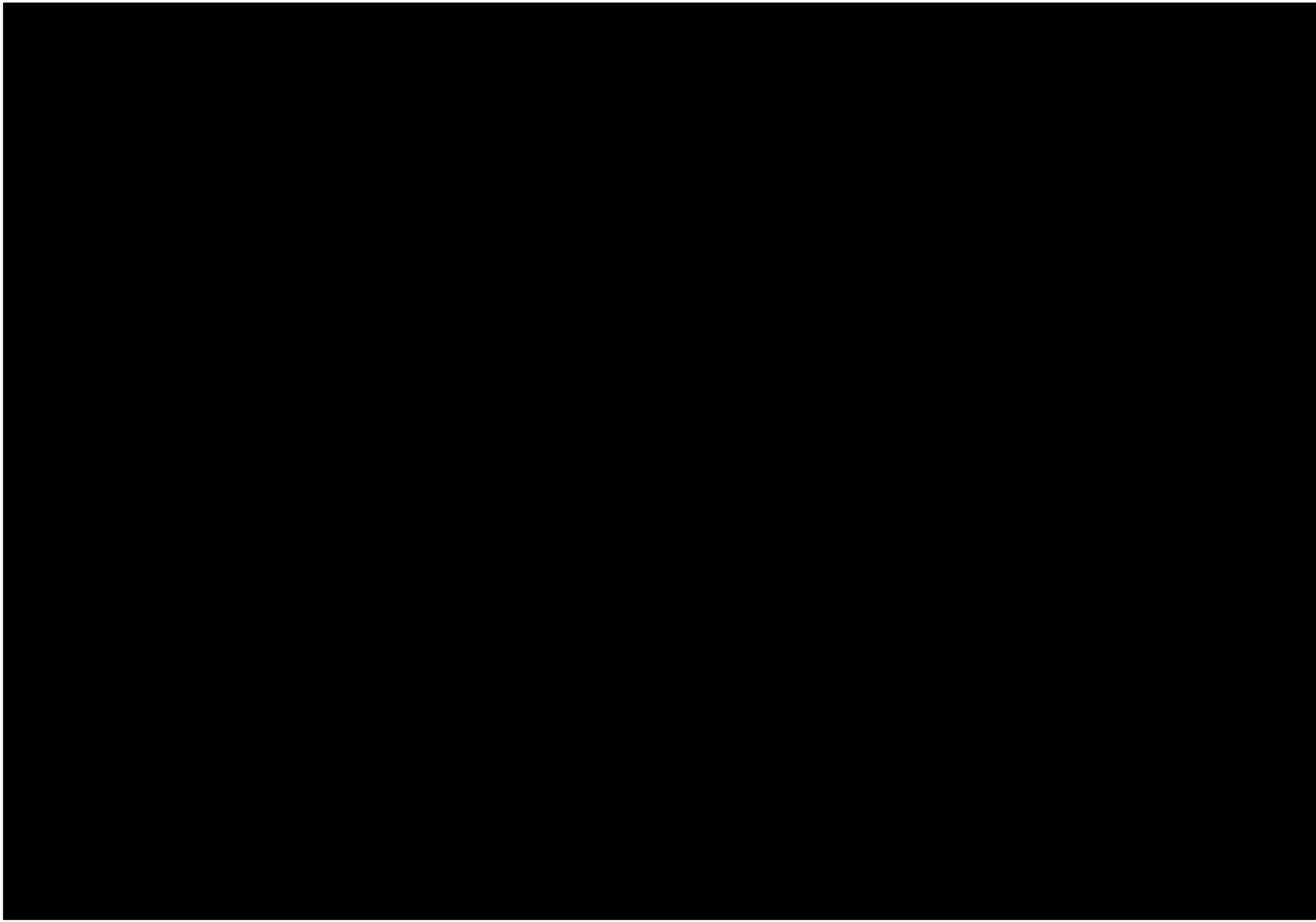


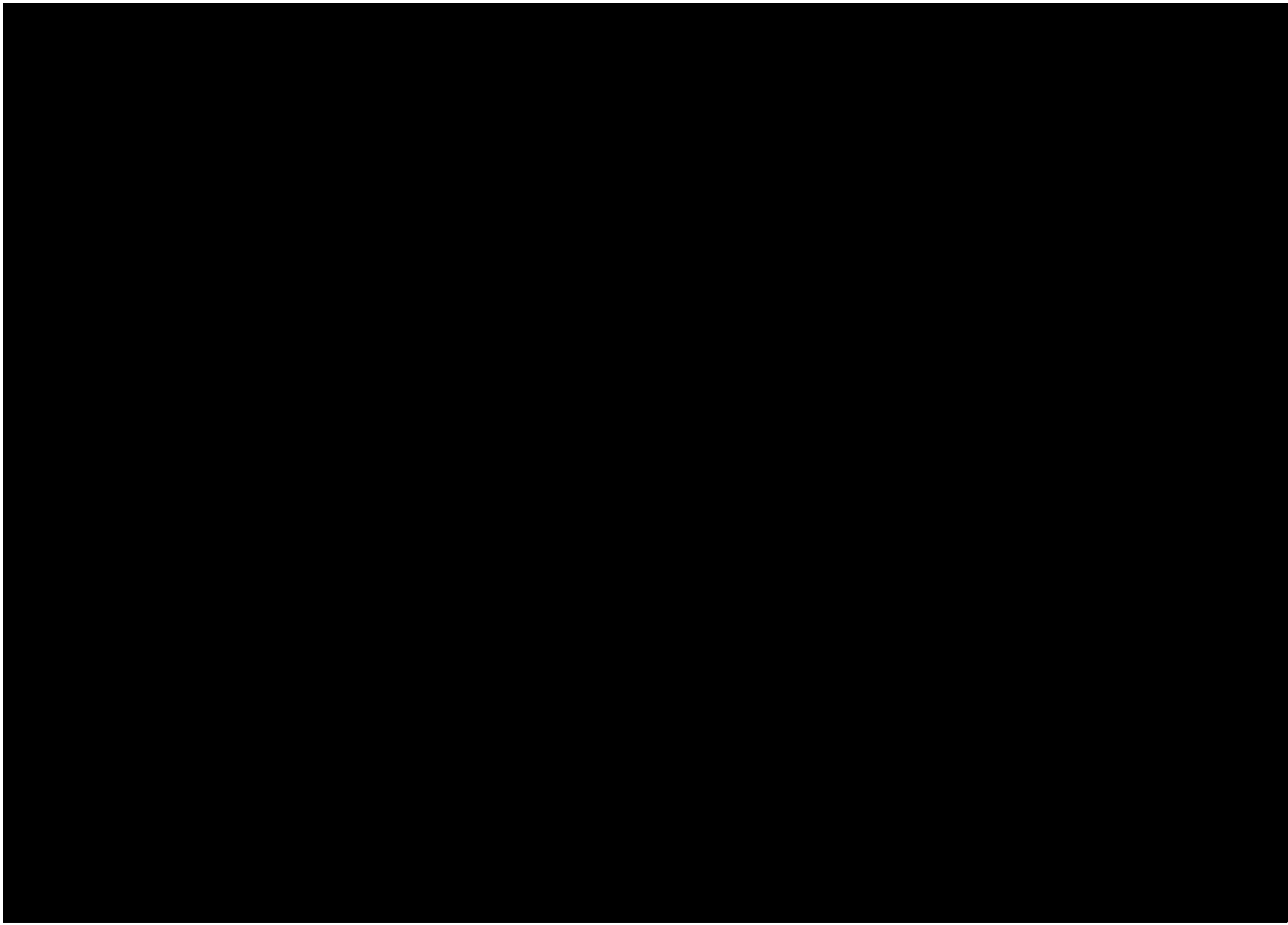


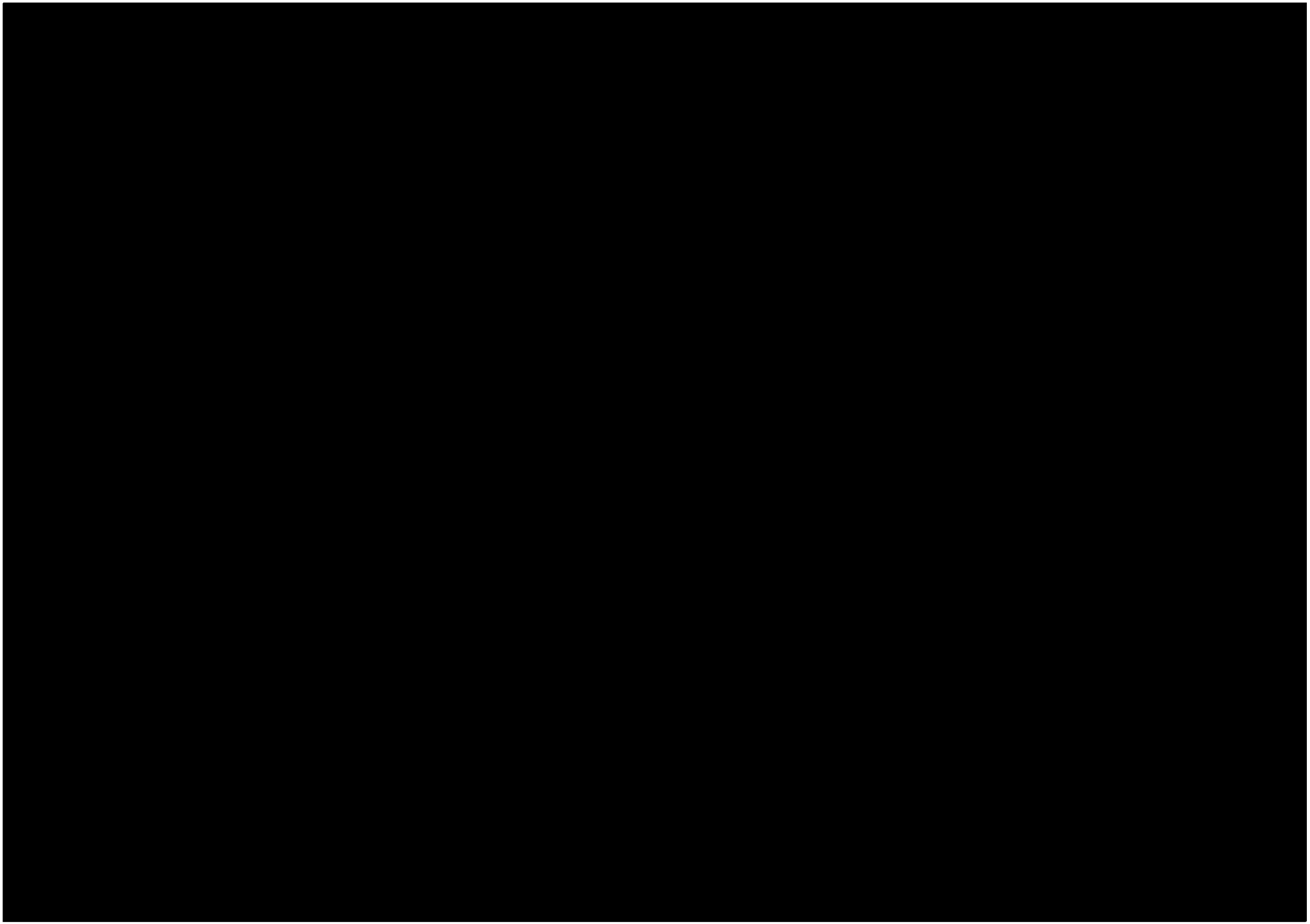


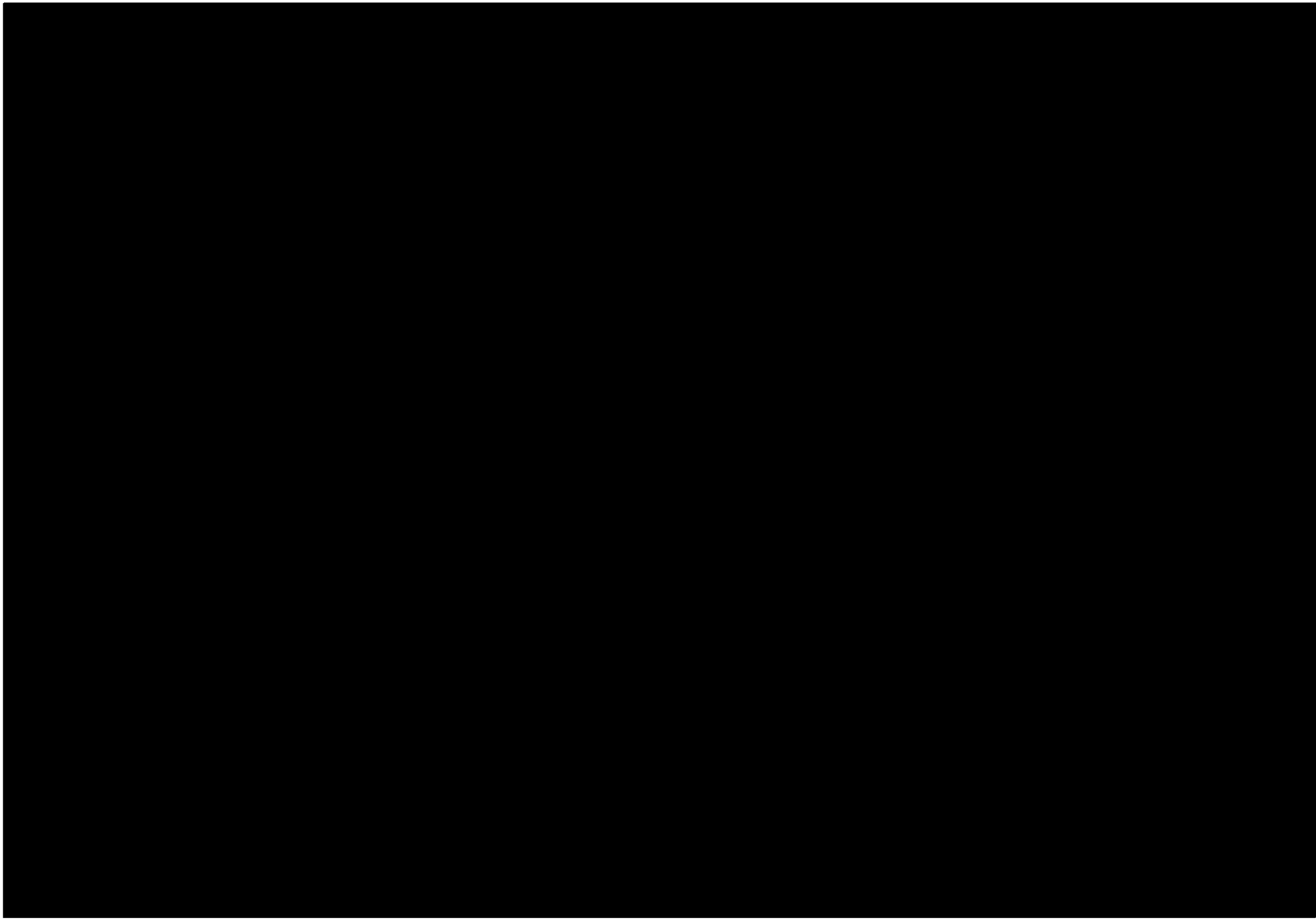


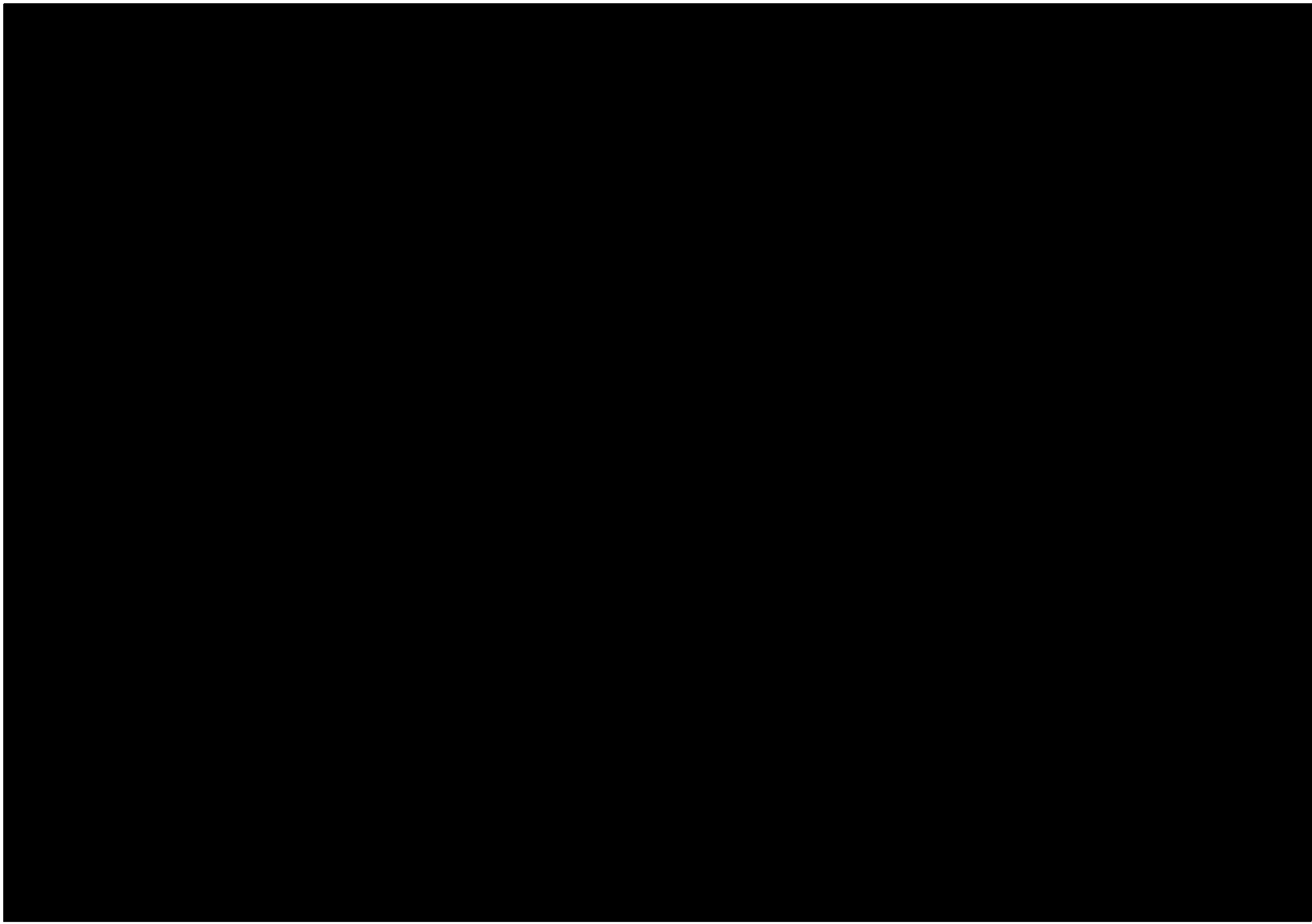


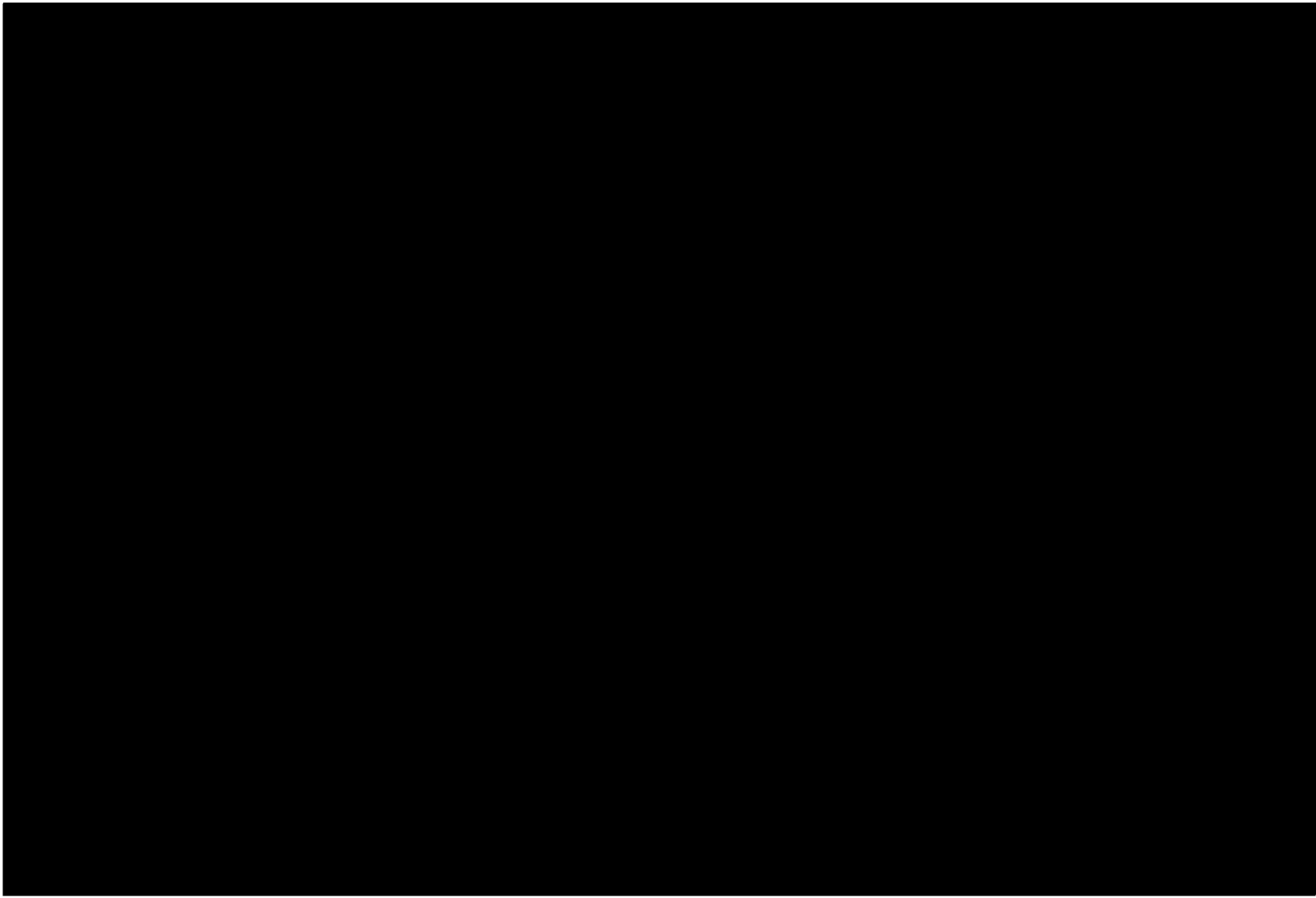


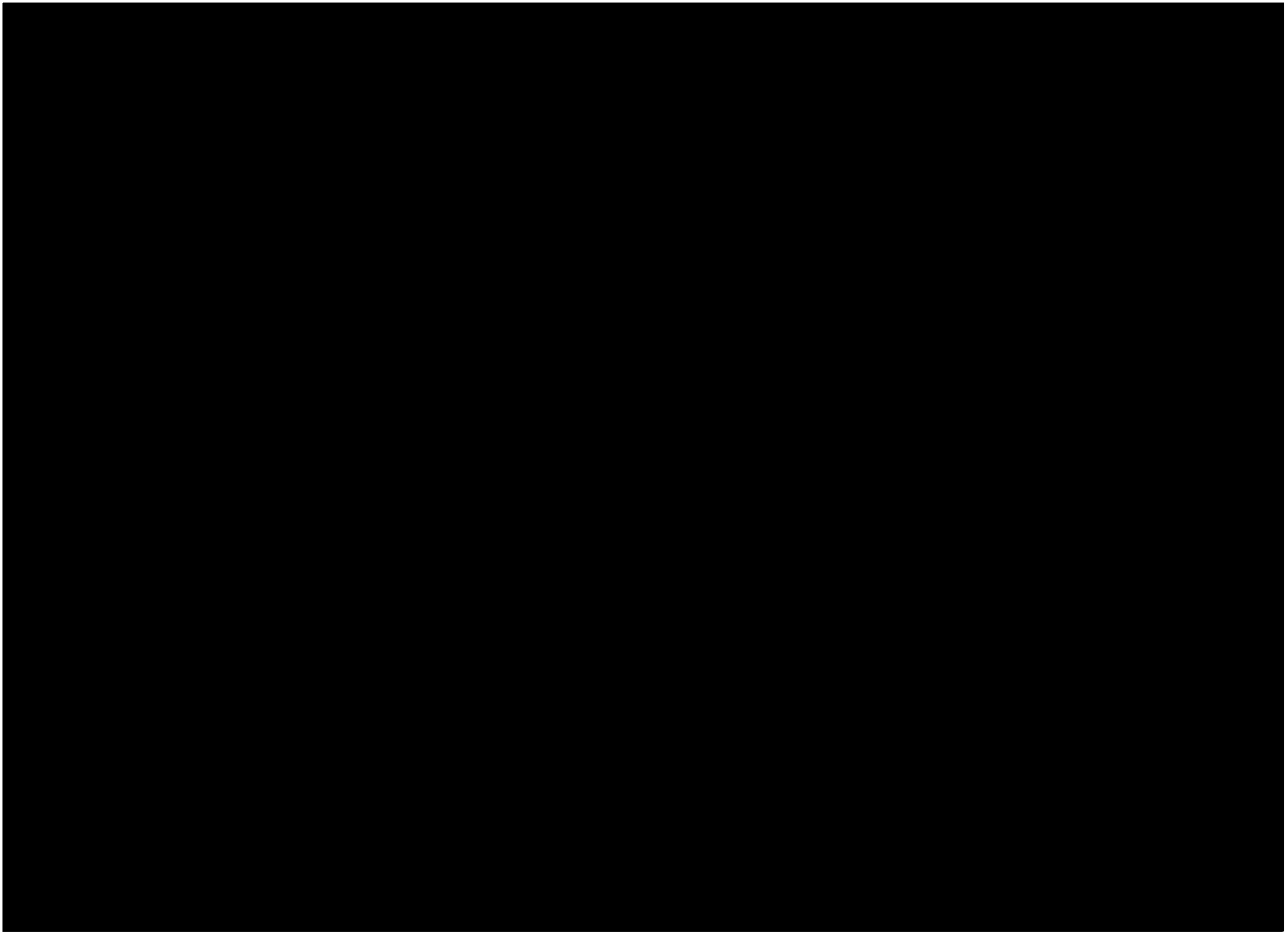


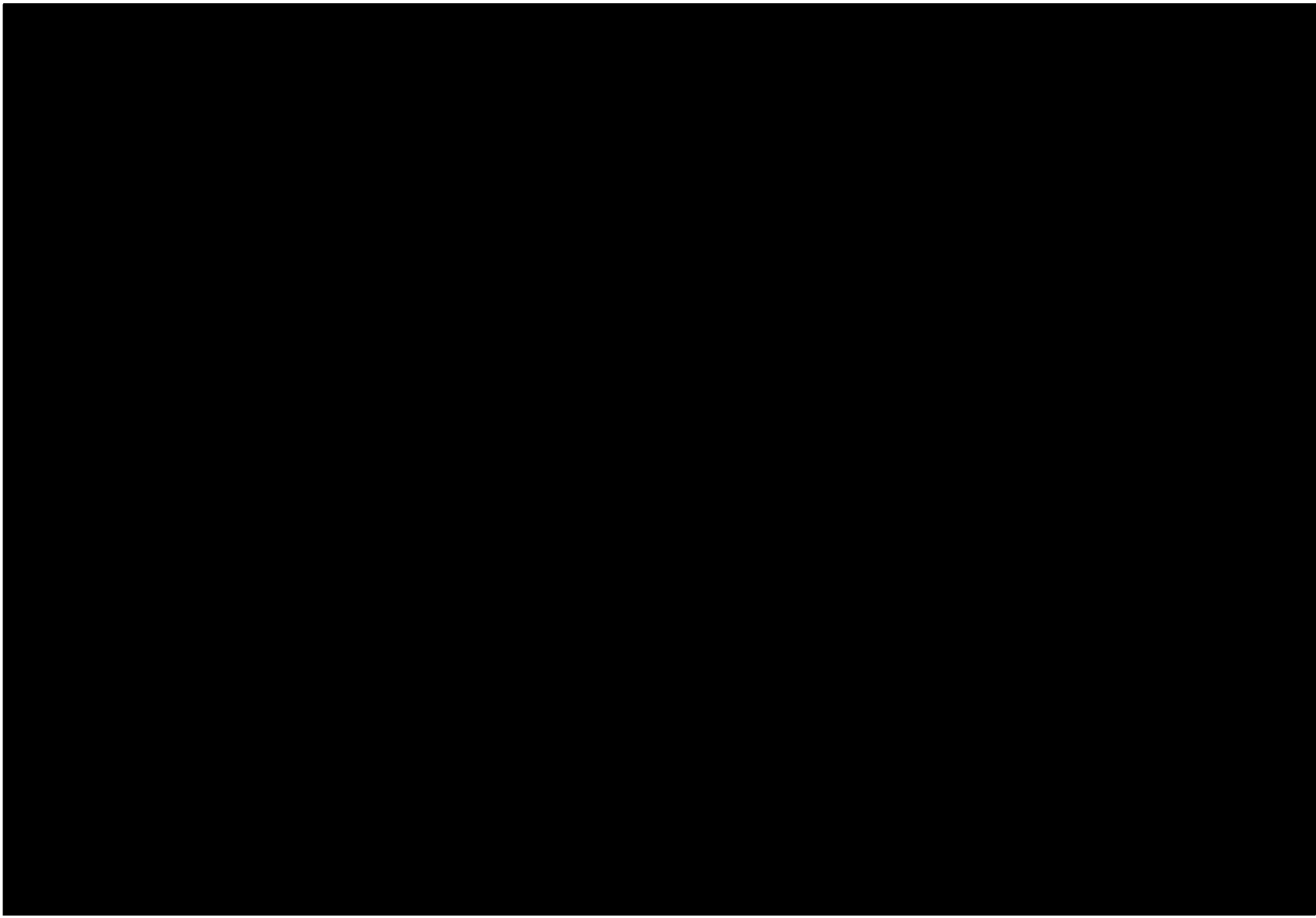


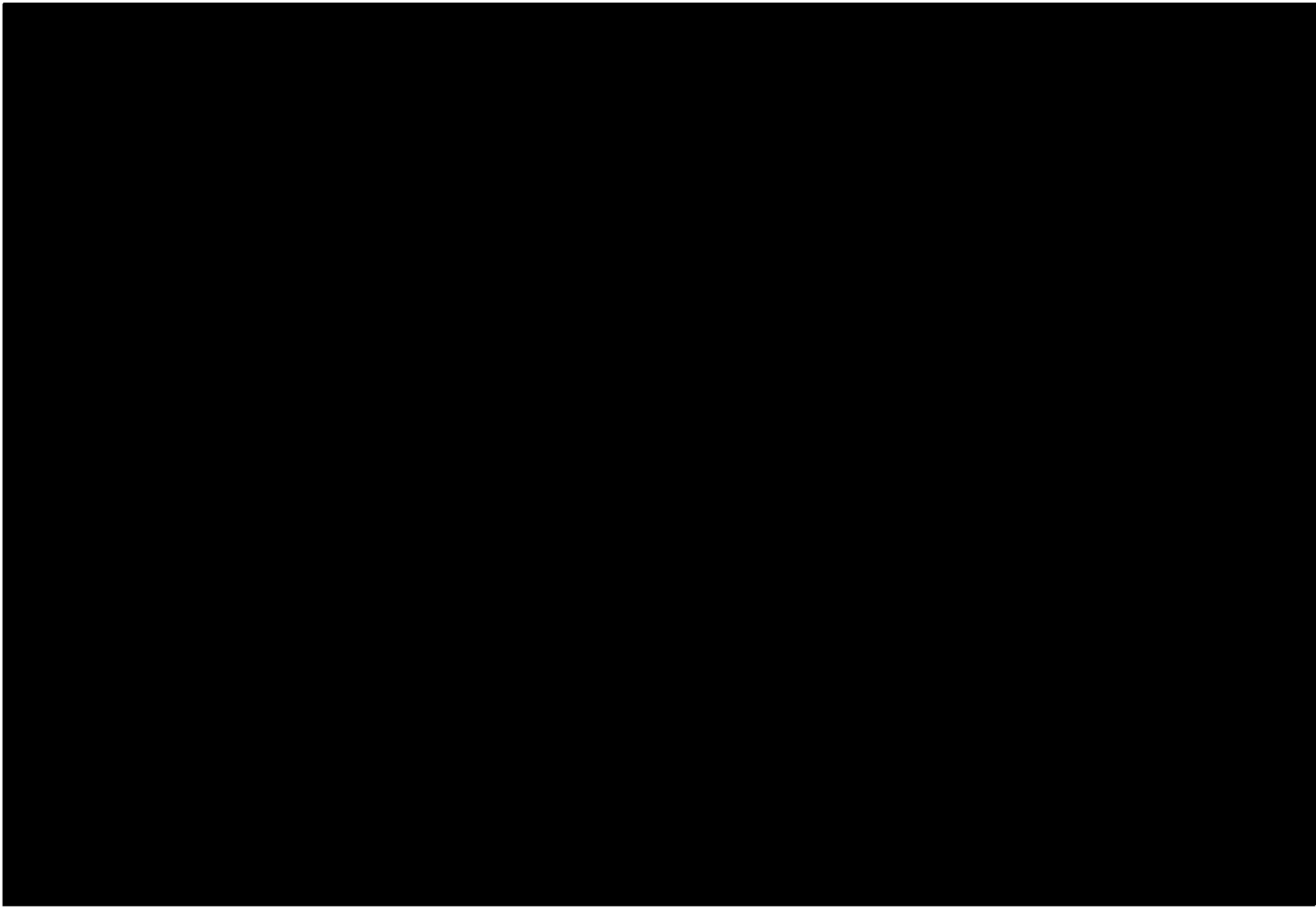


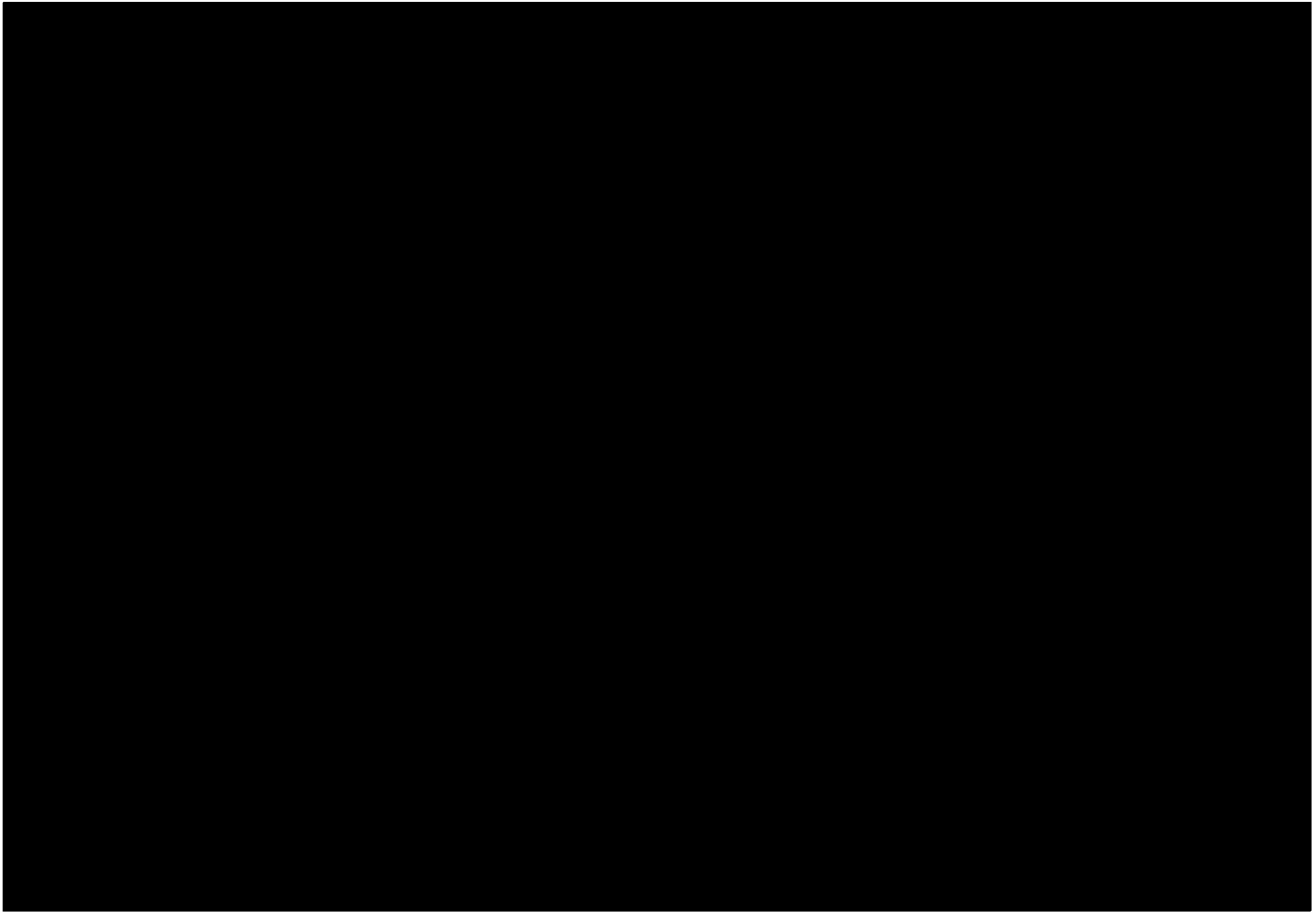


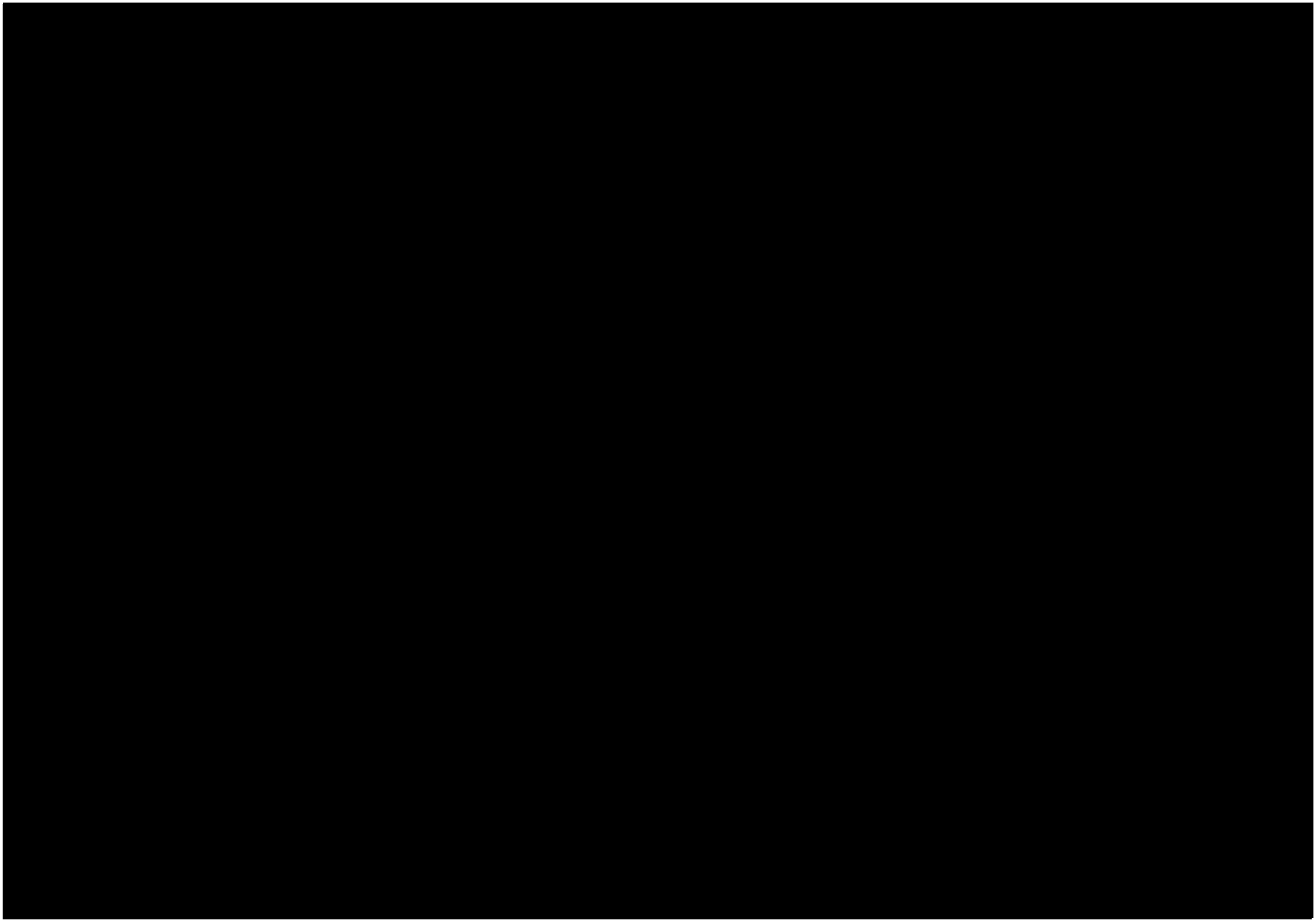


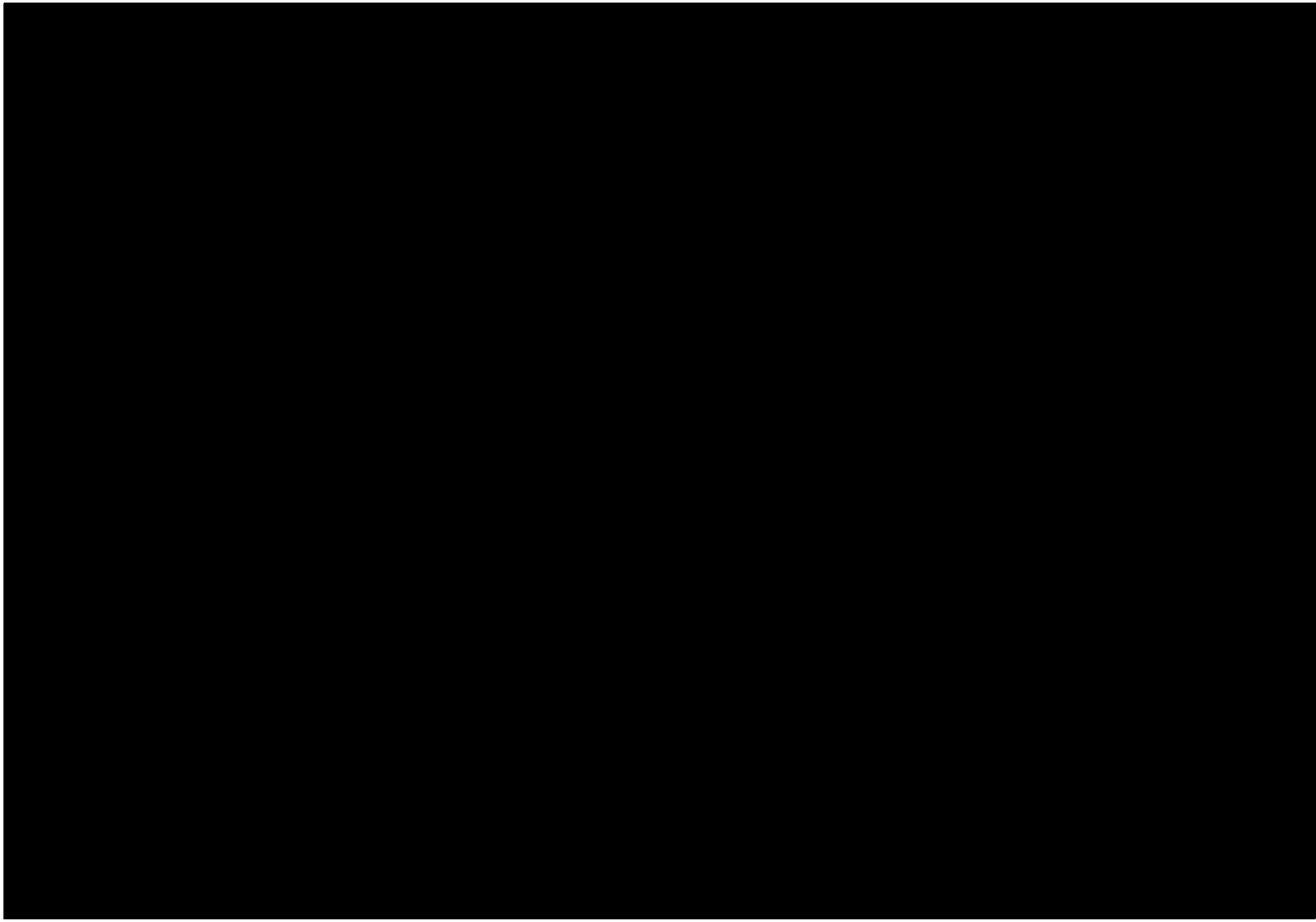


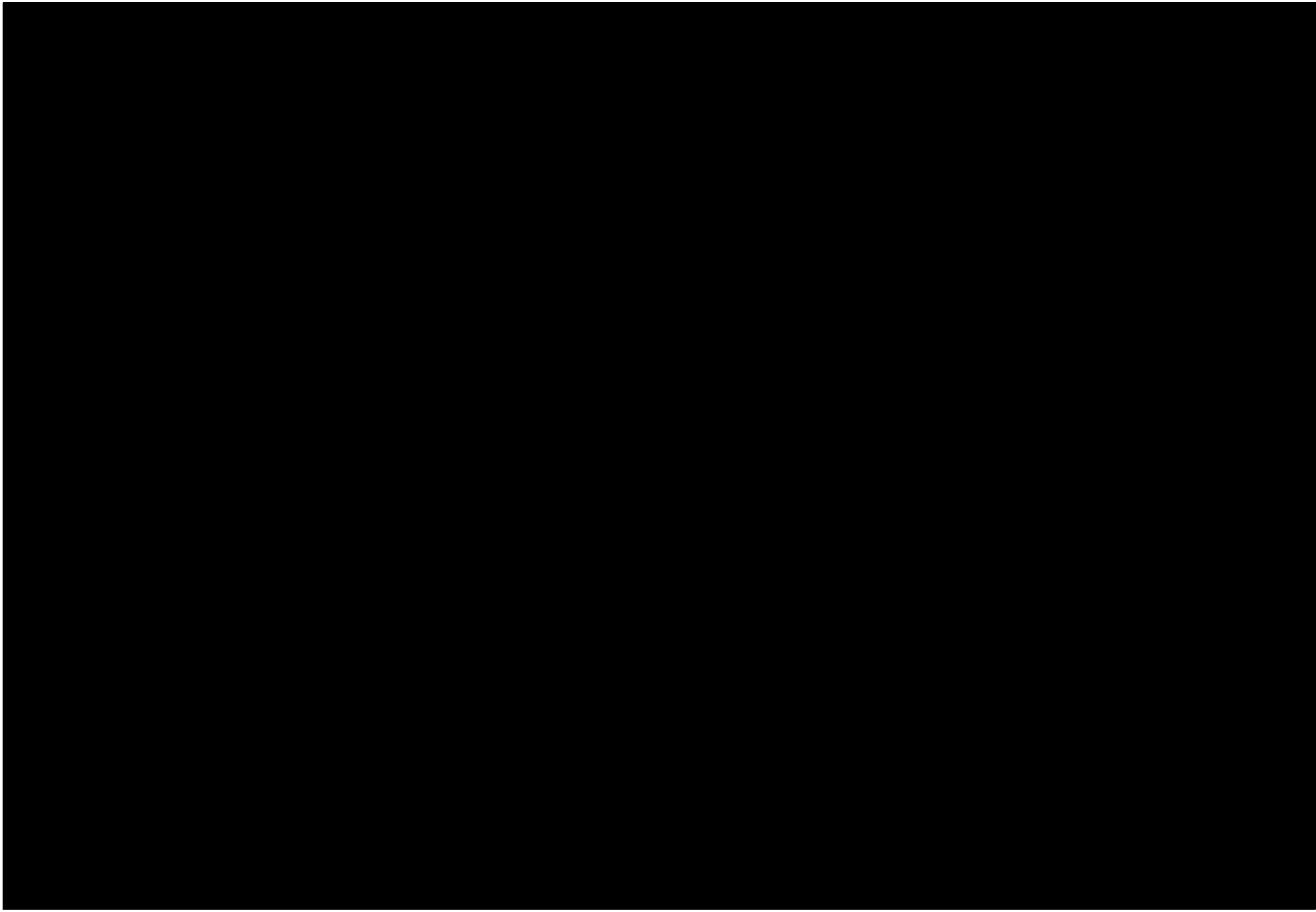


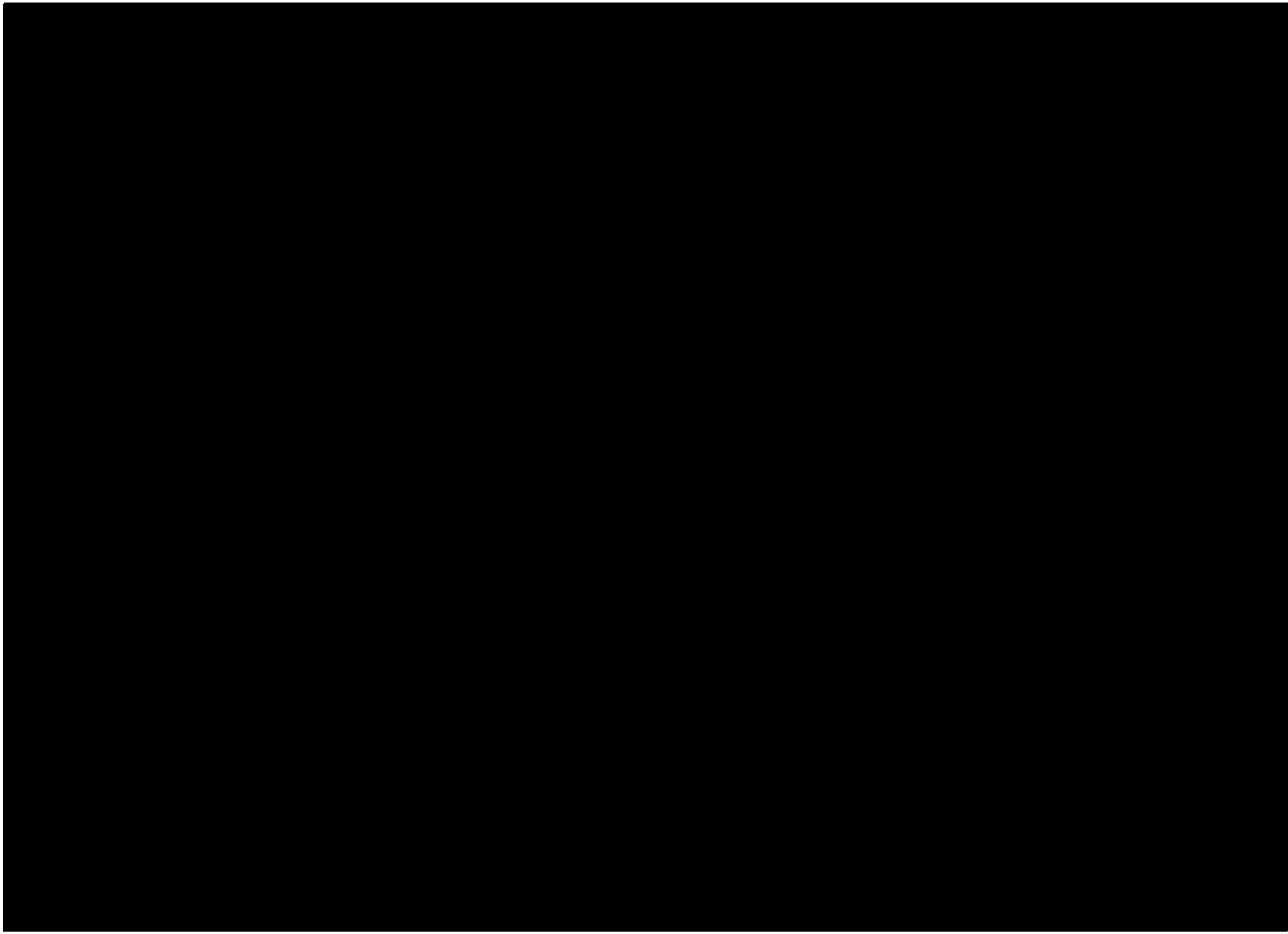


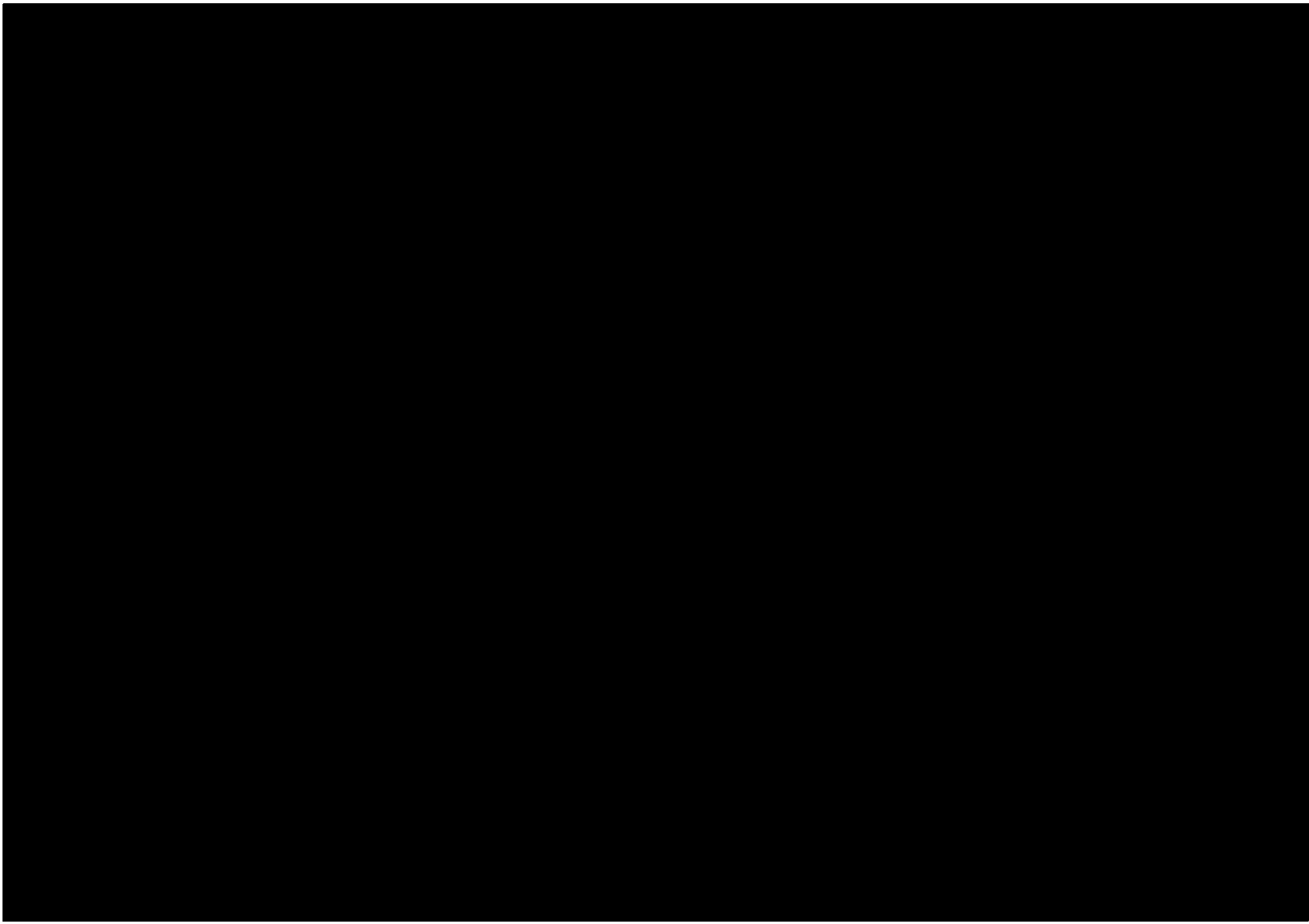


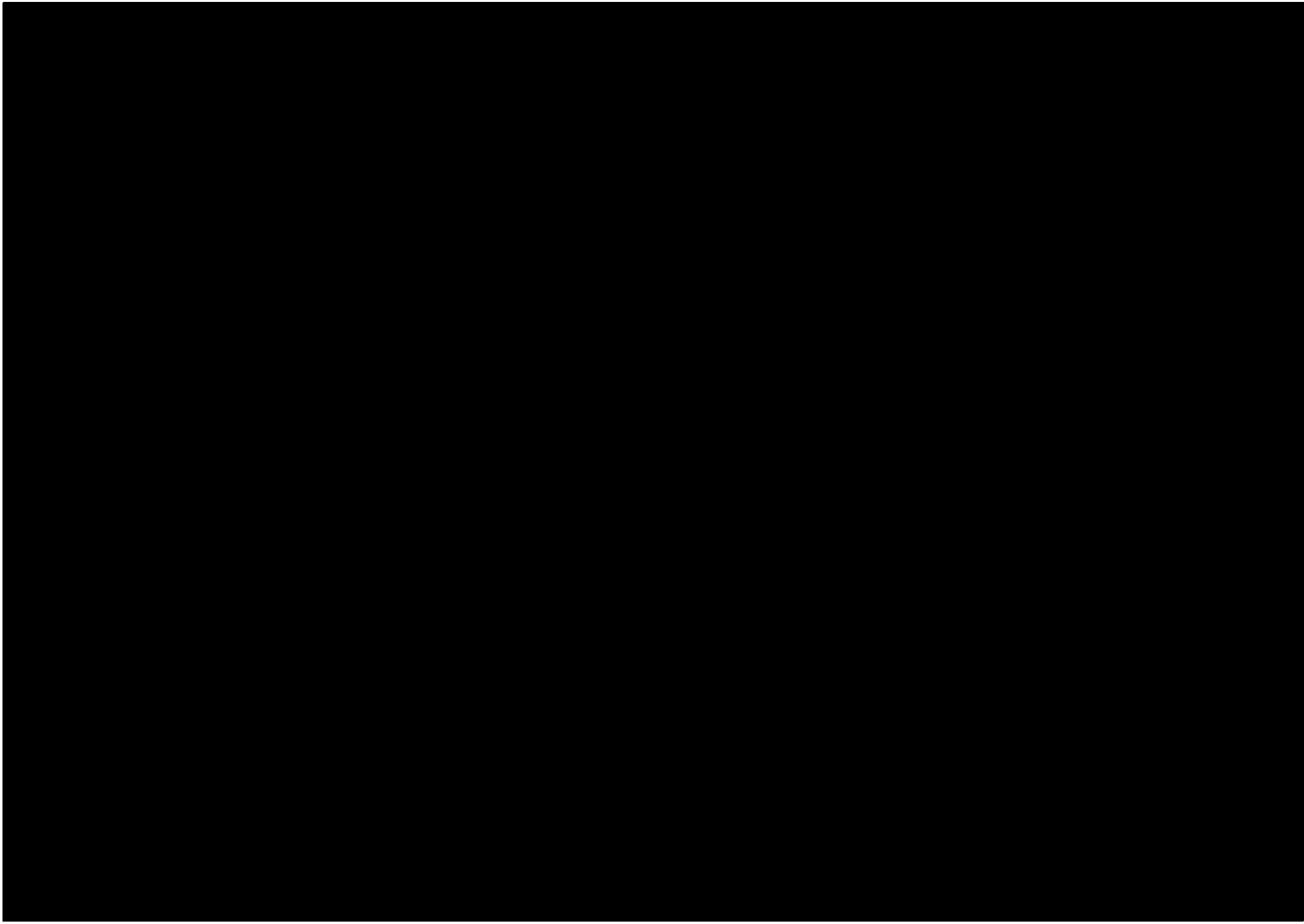












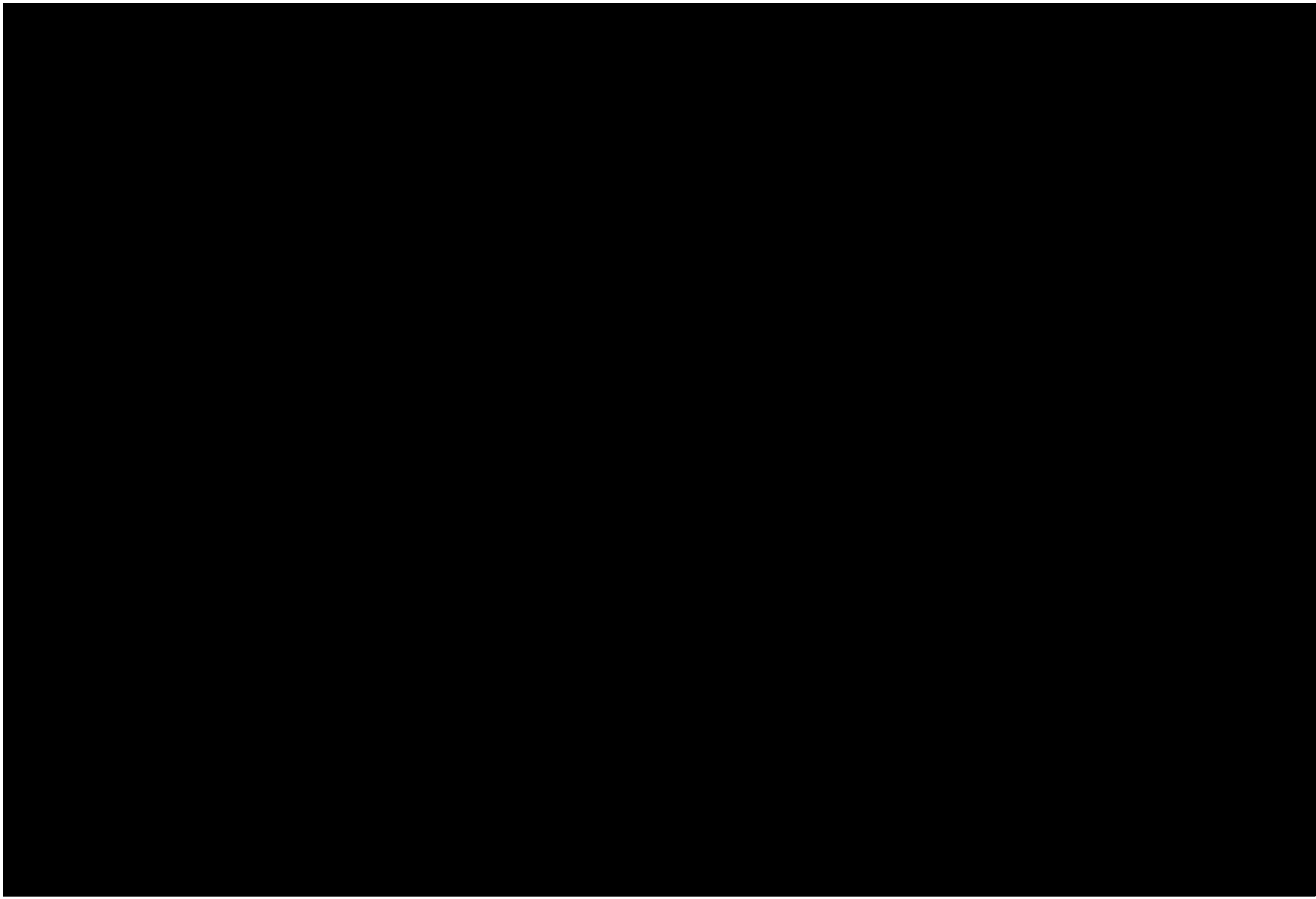
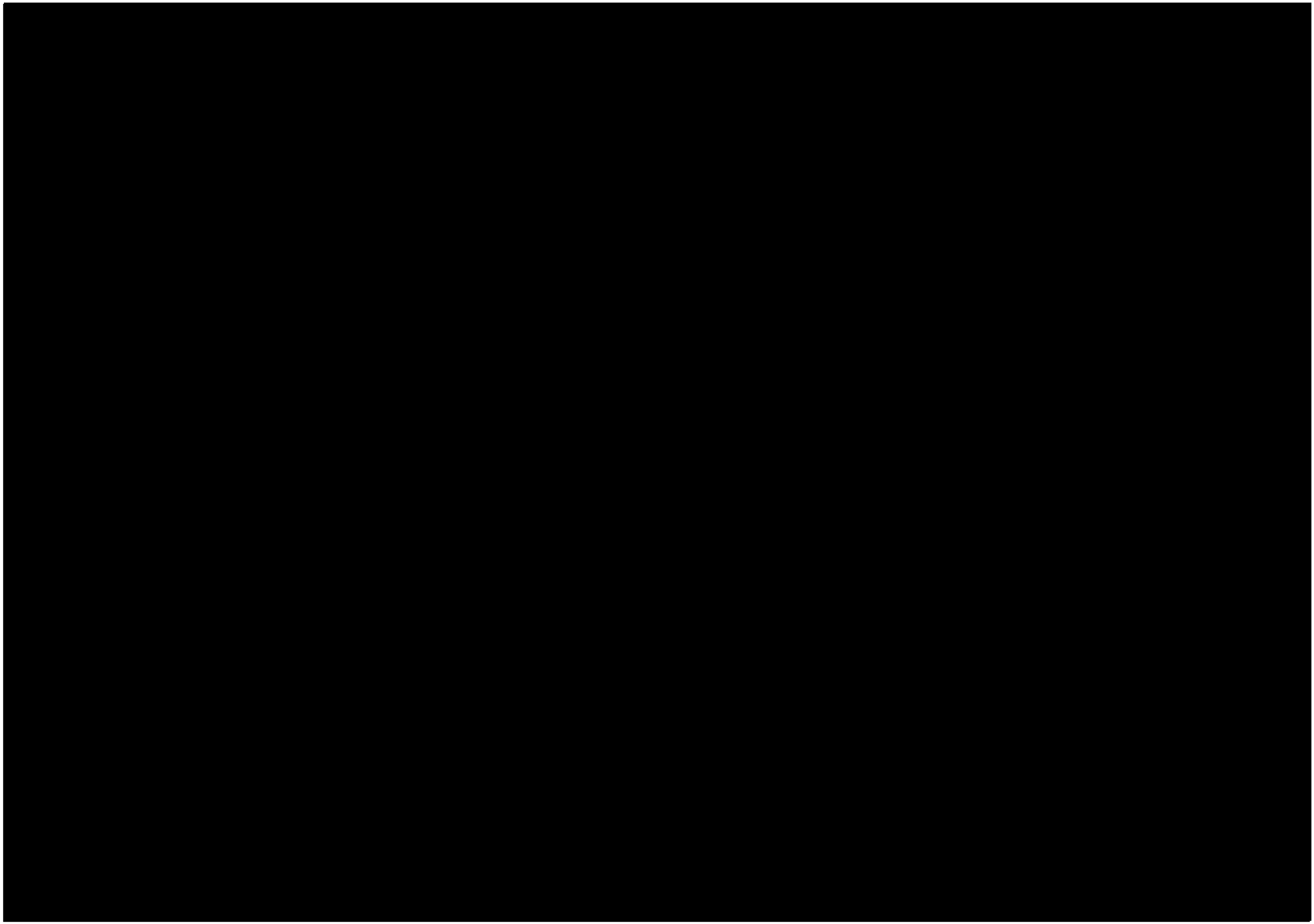
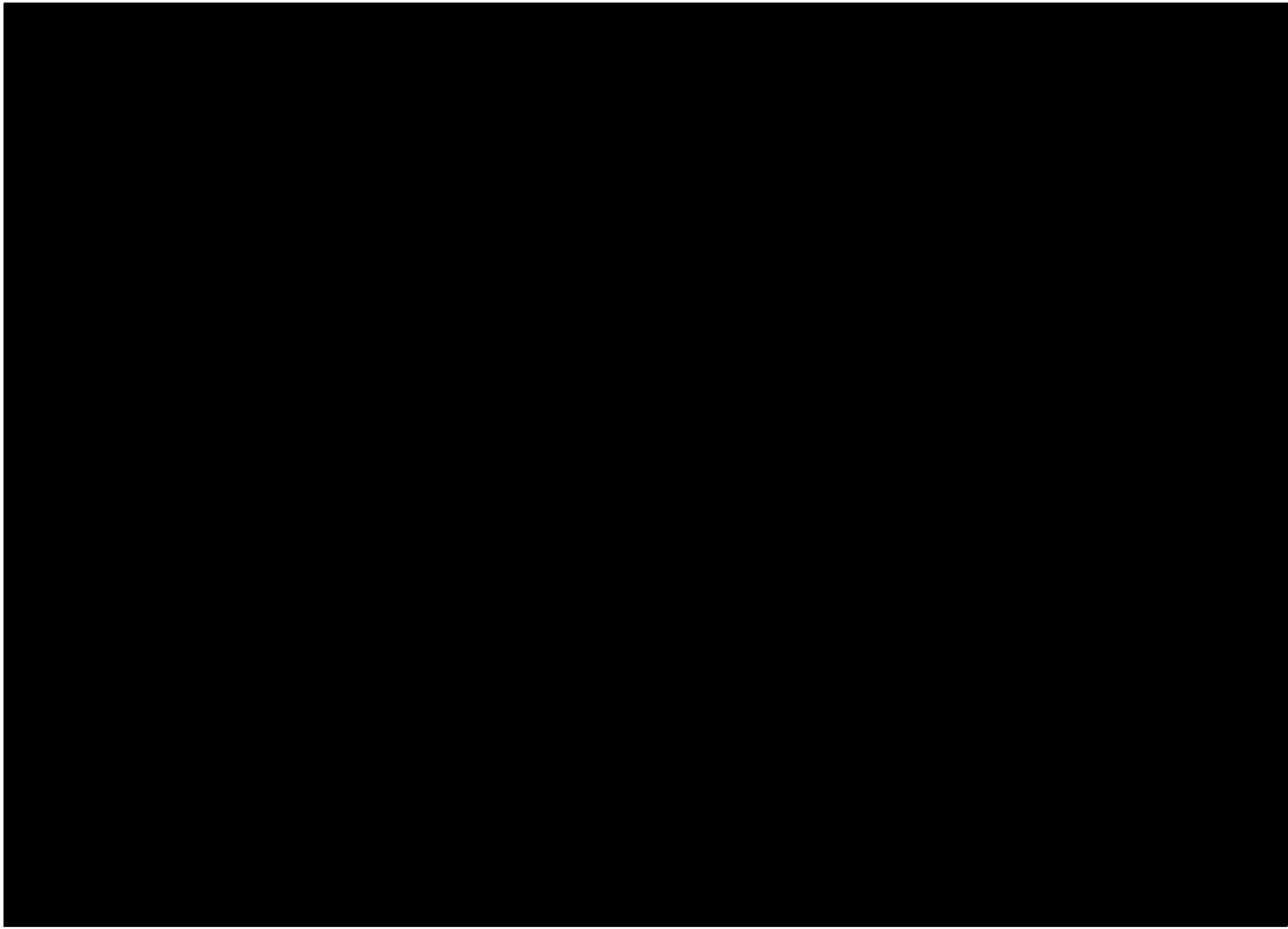
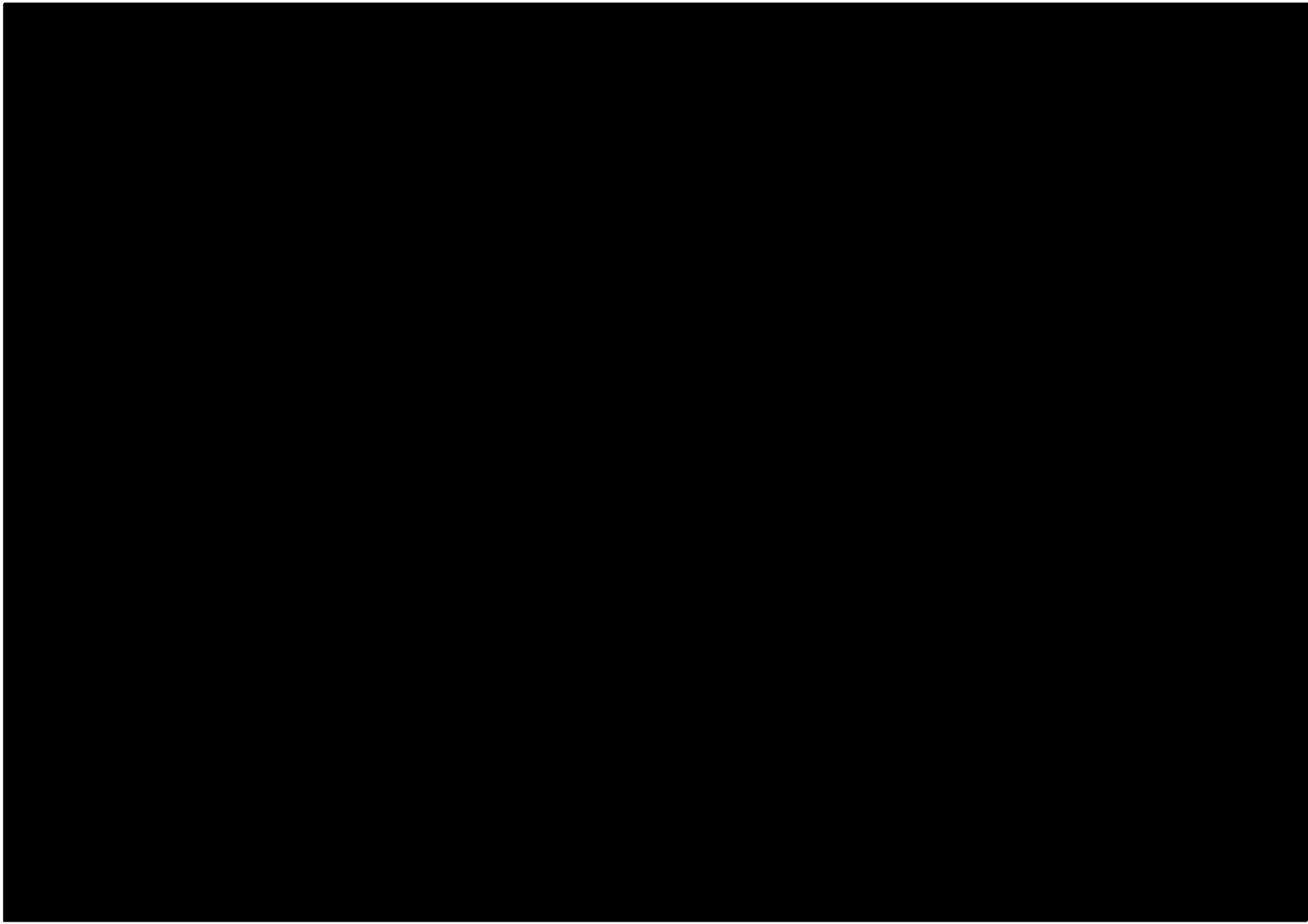
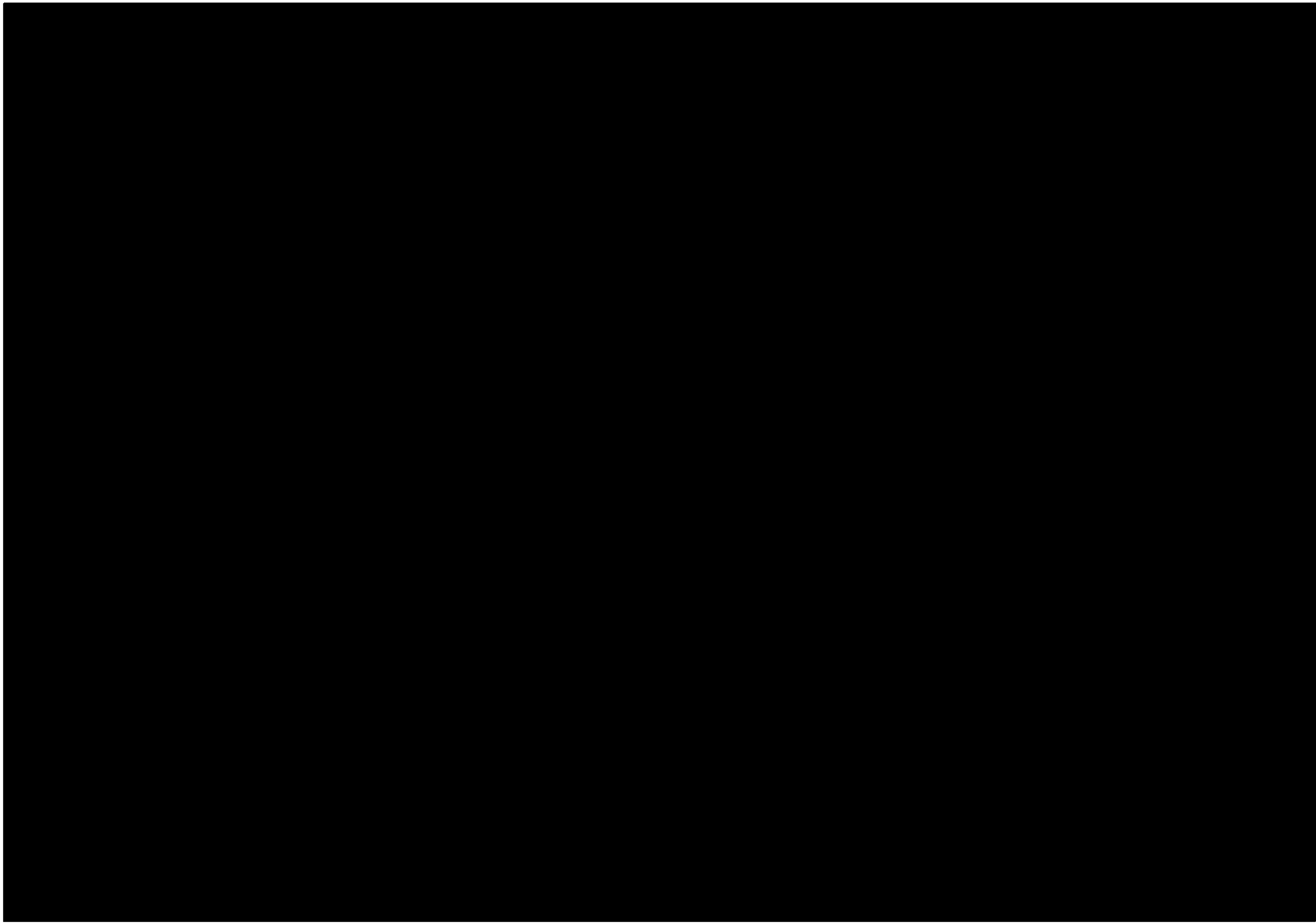


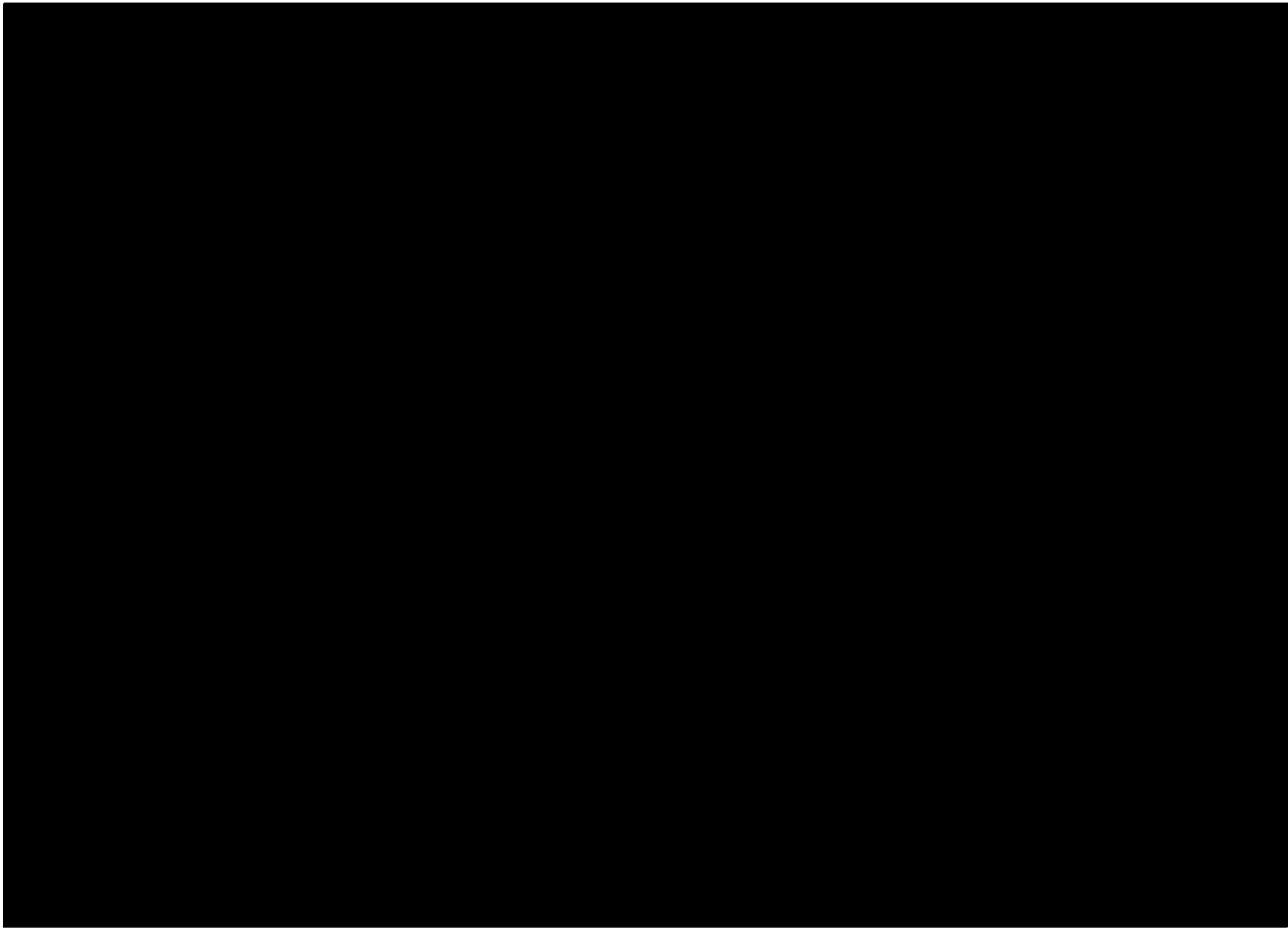
EXHIBIT F

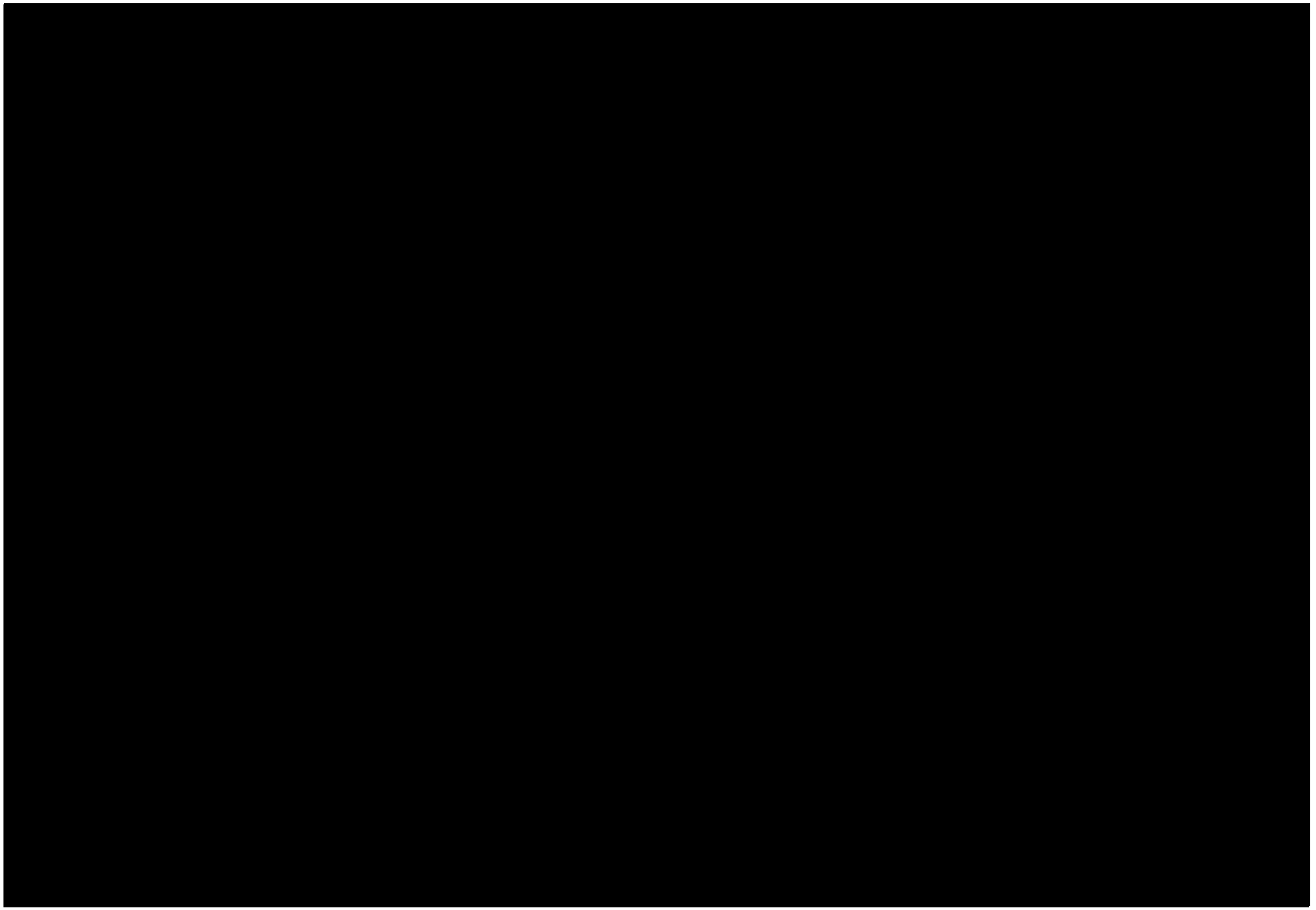


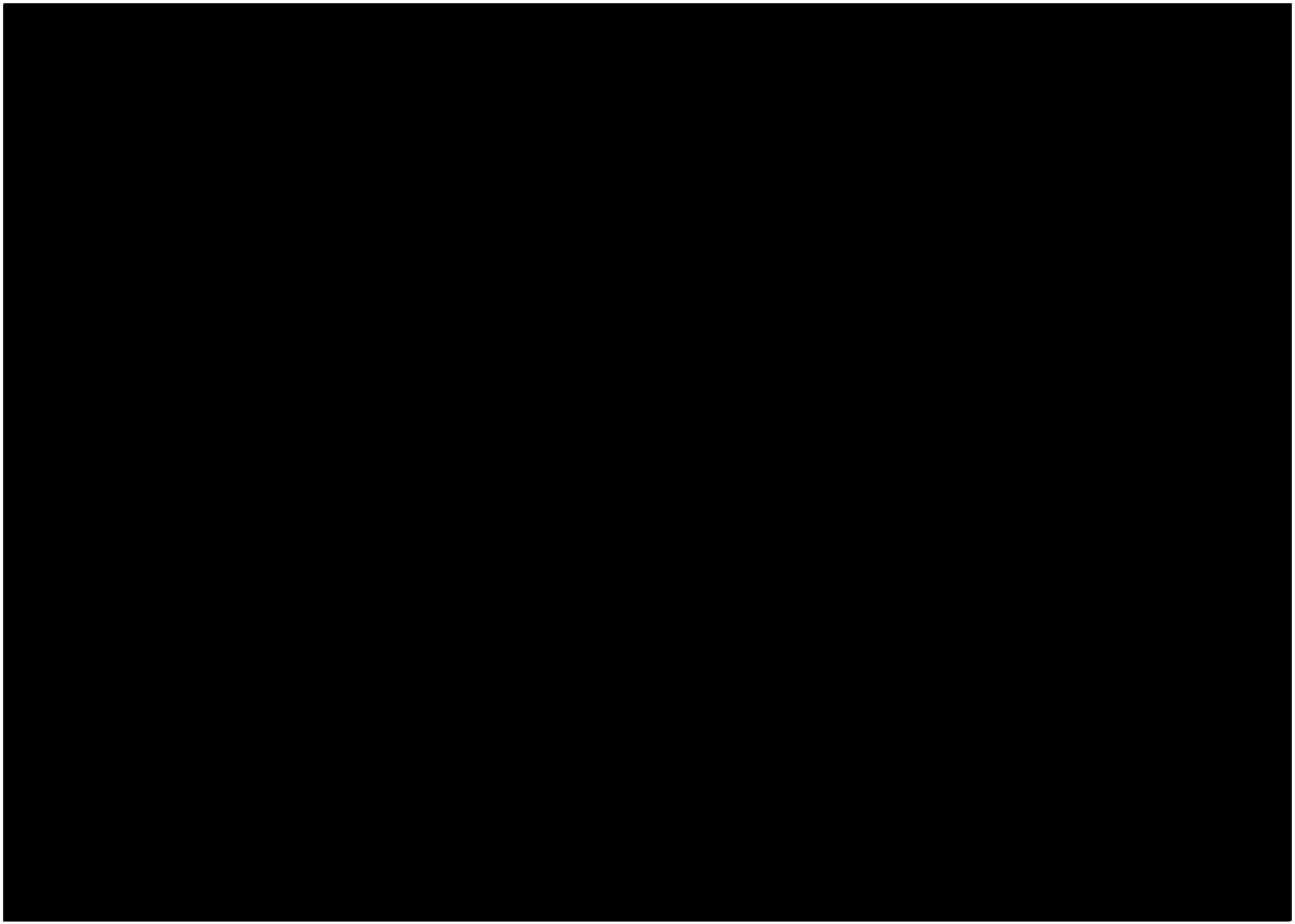


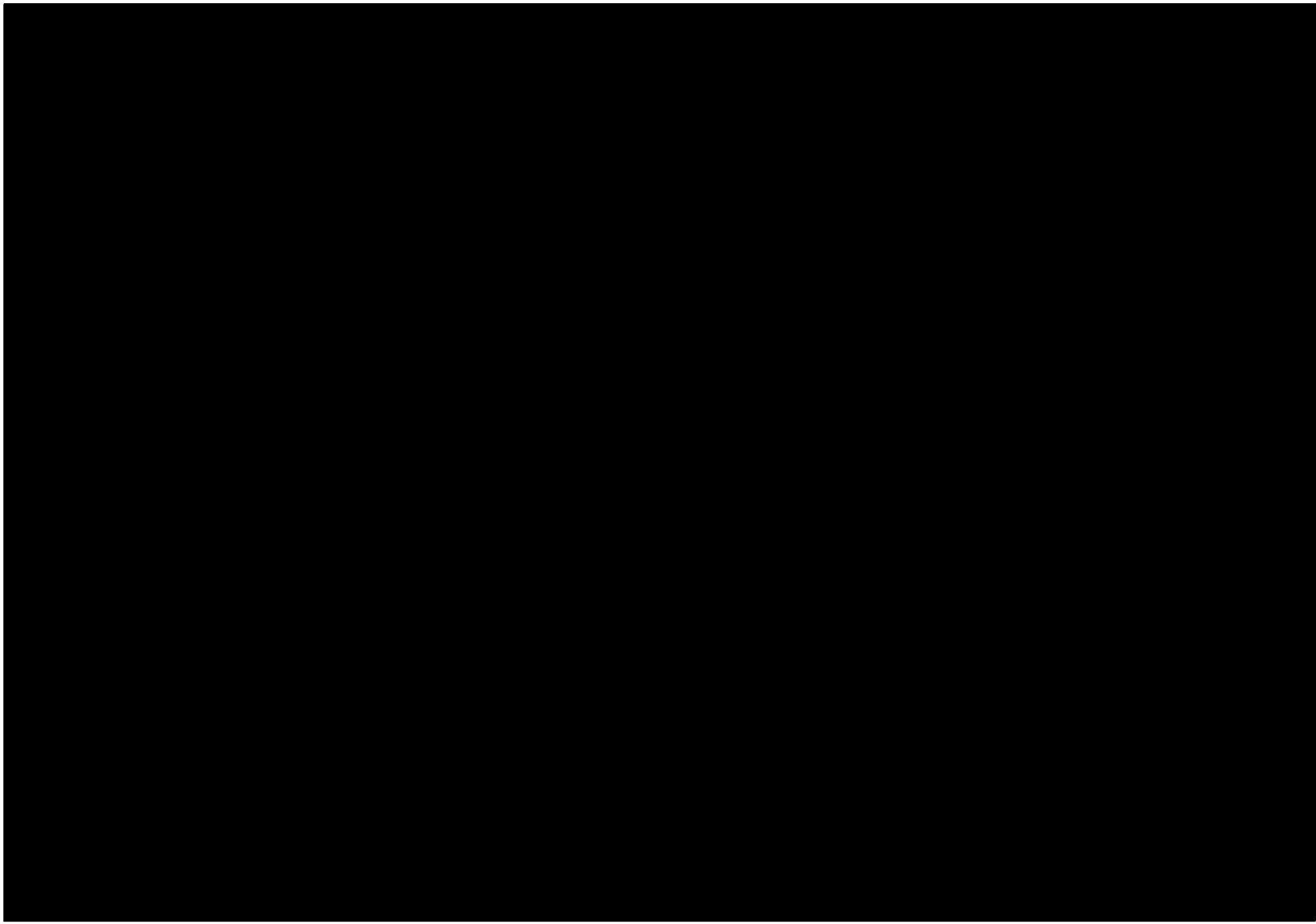


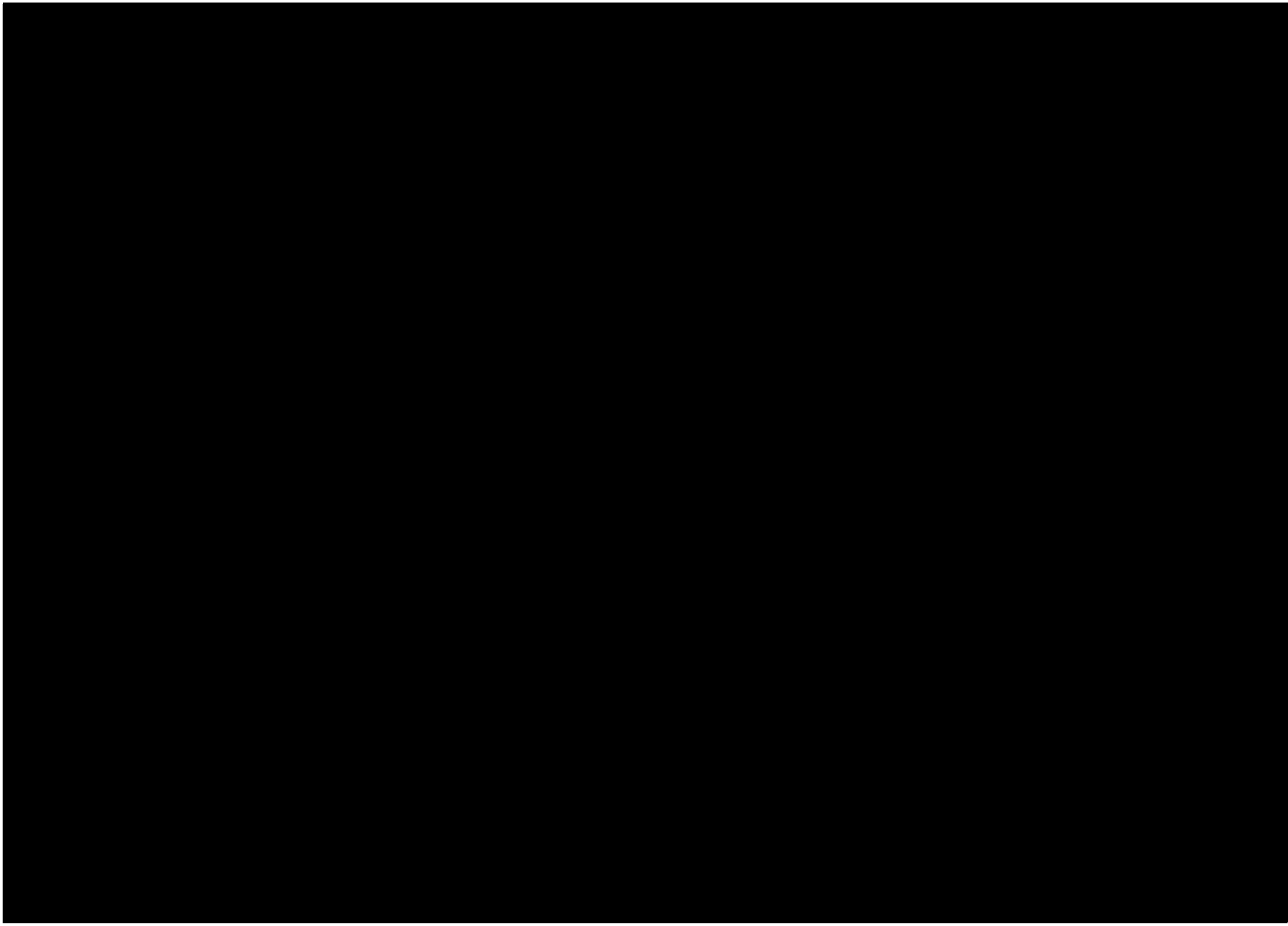


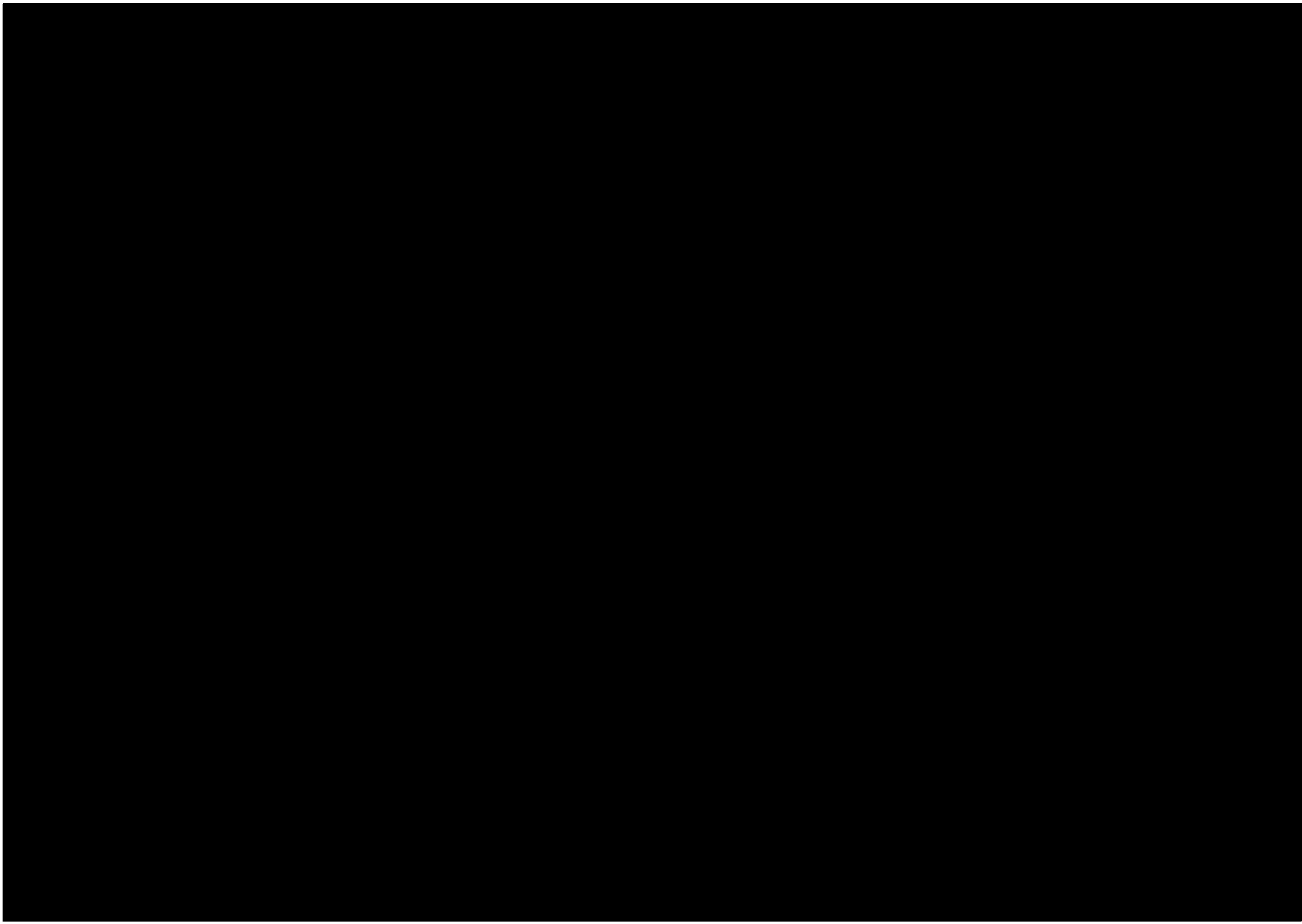


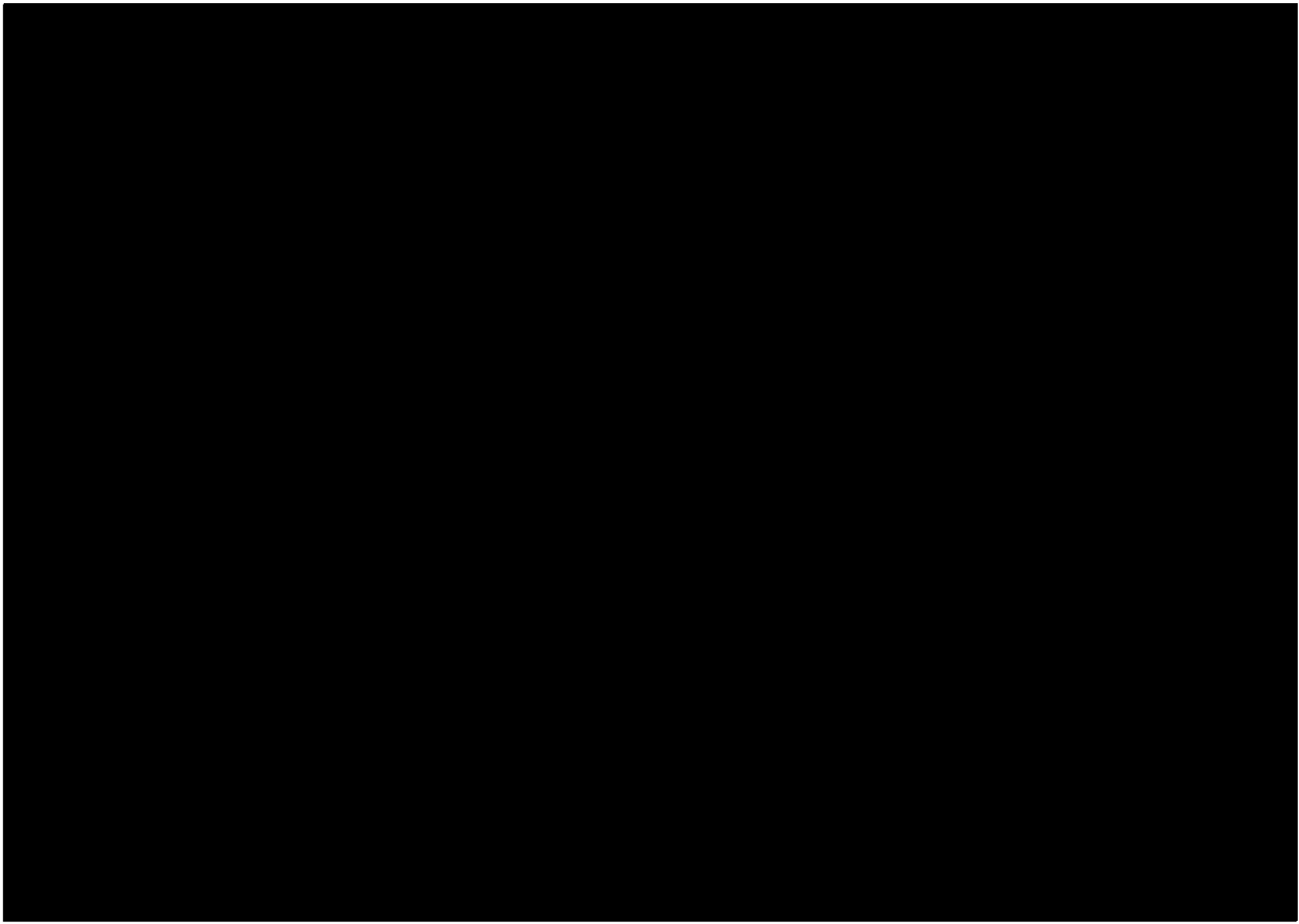


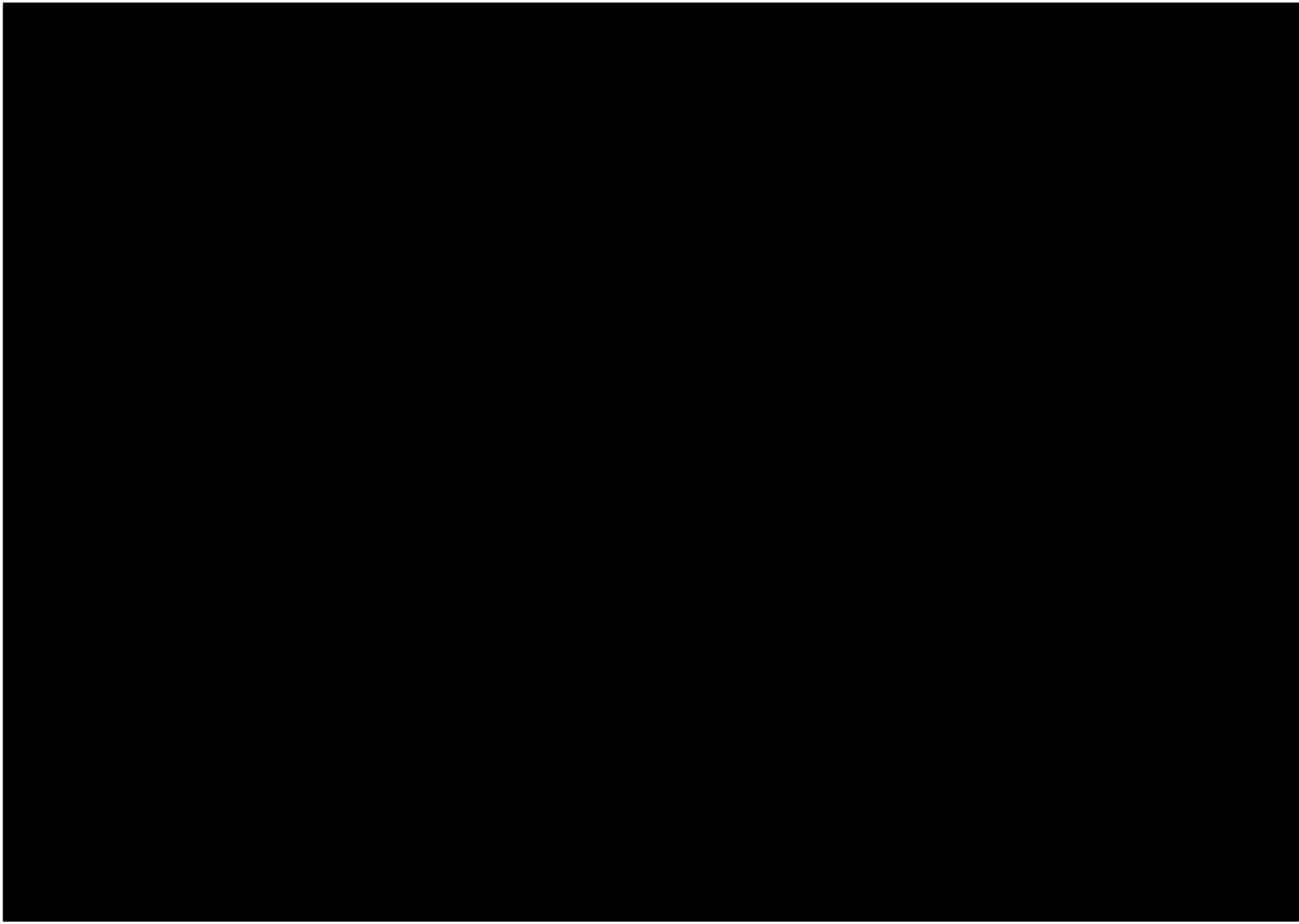


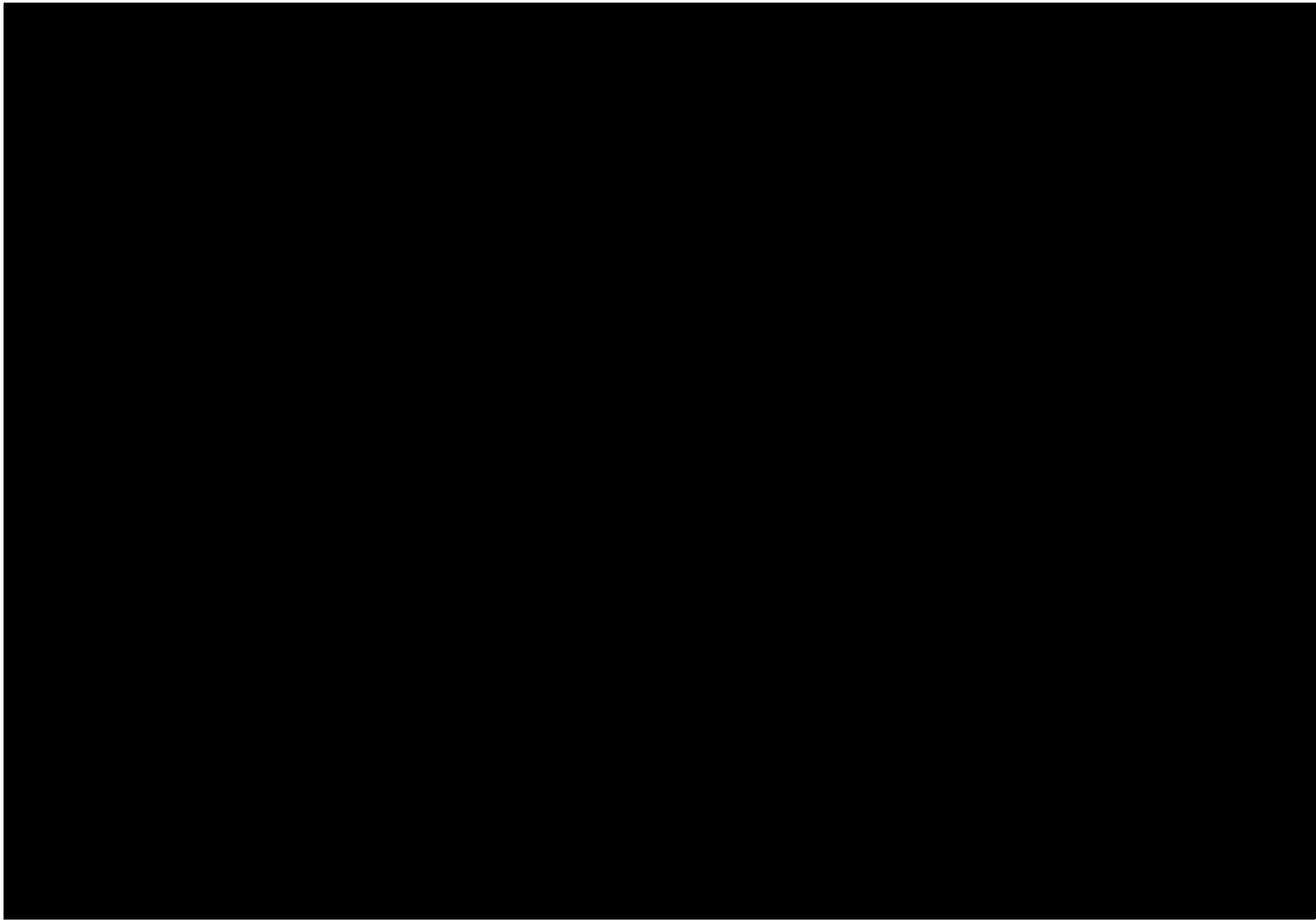


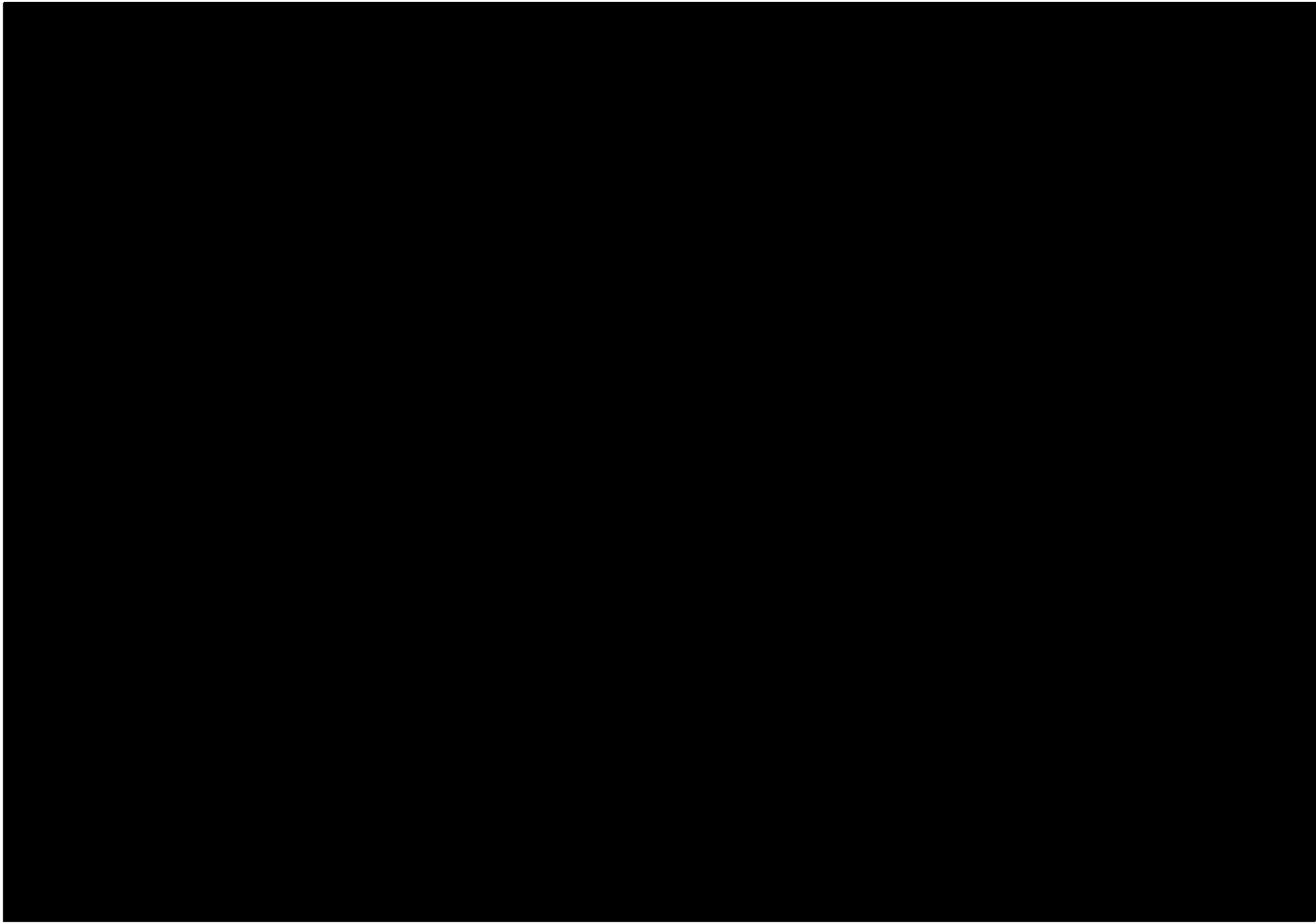


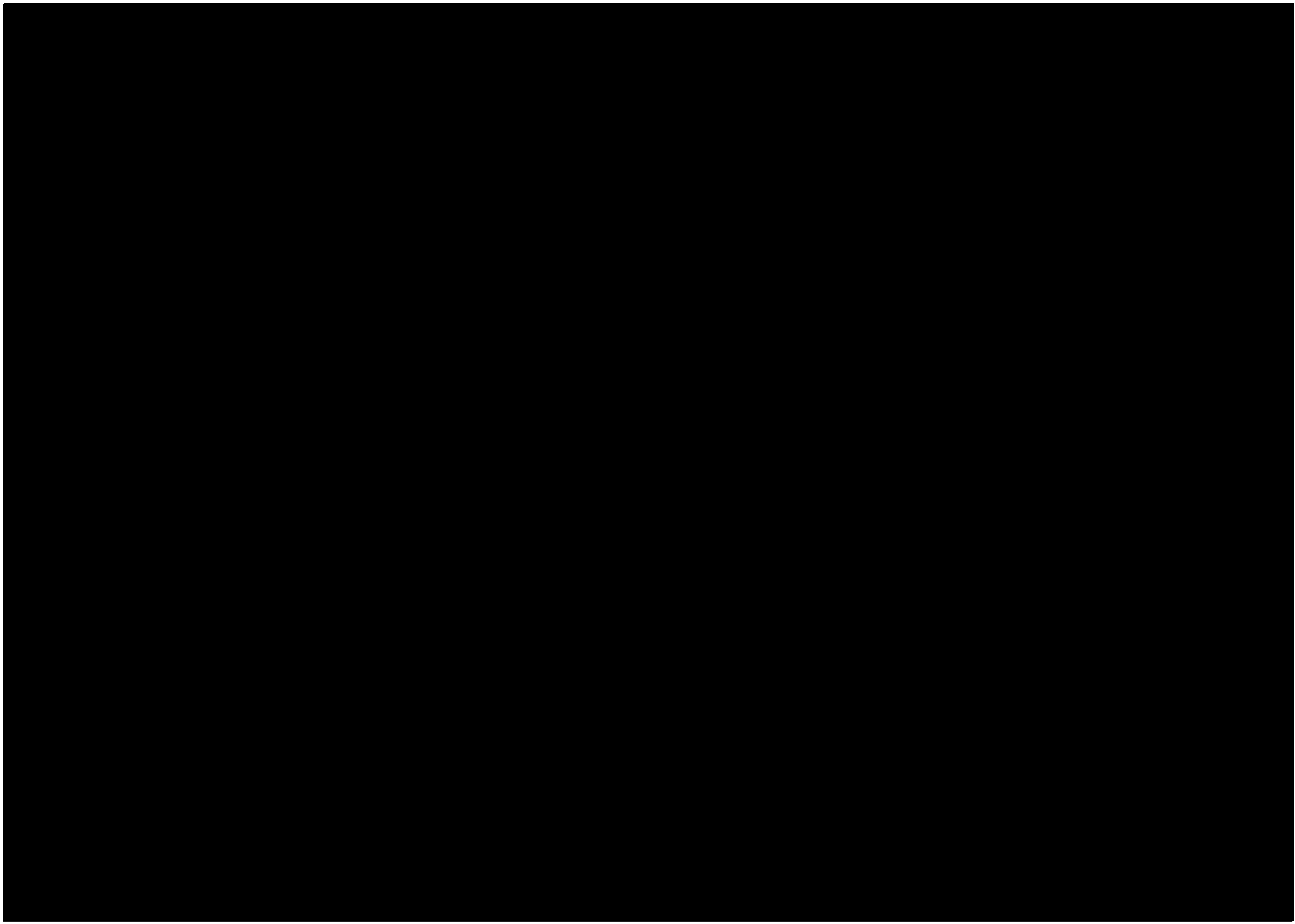


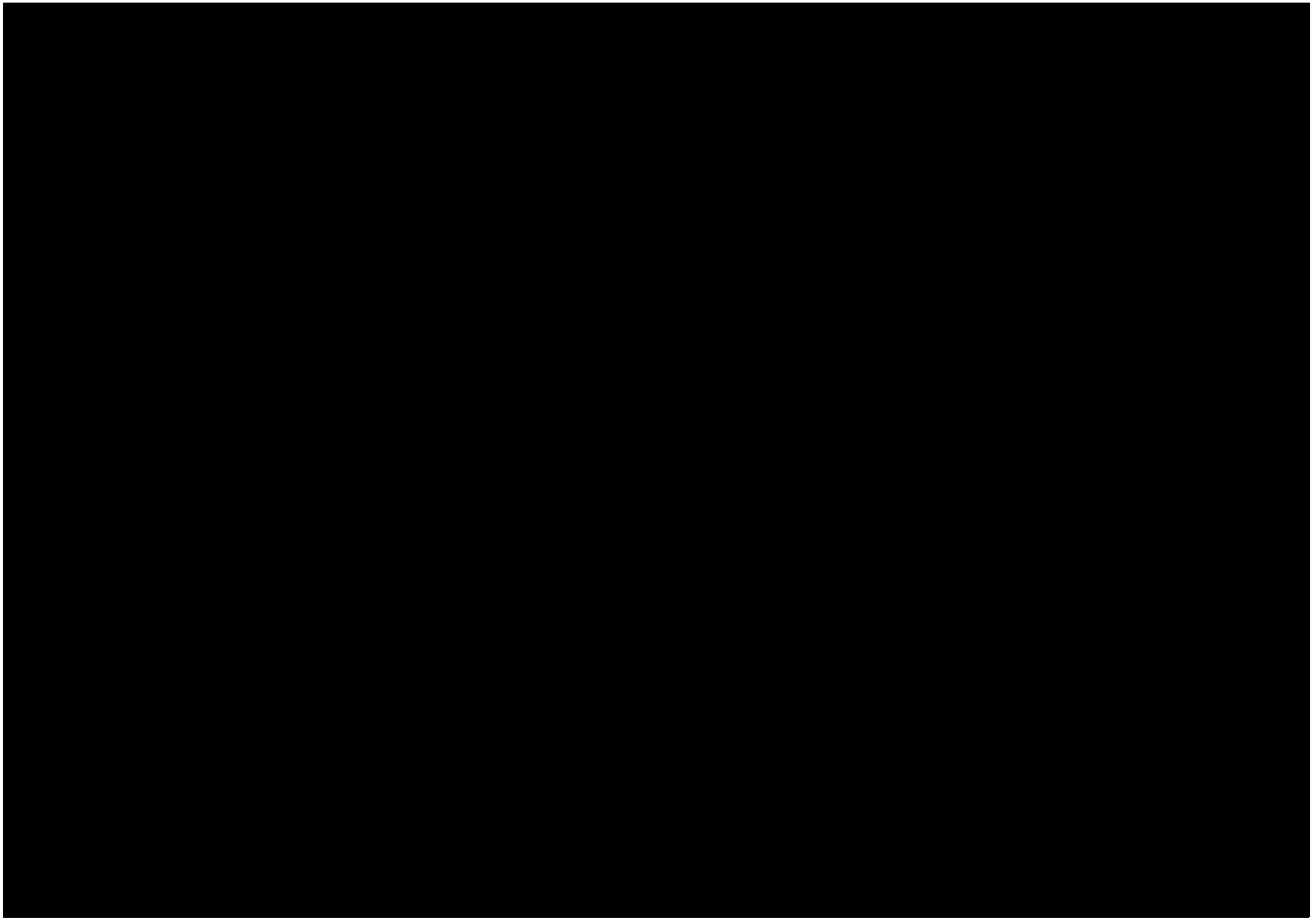


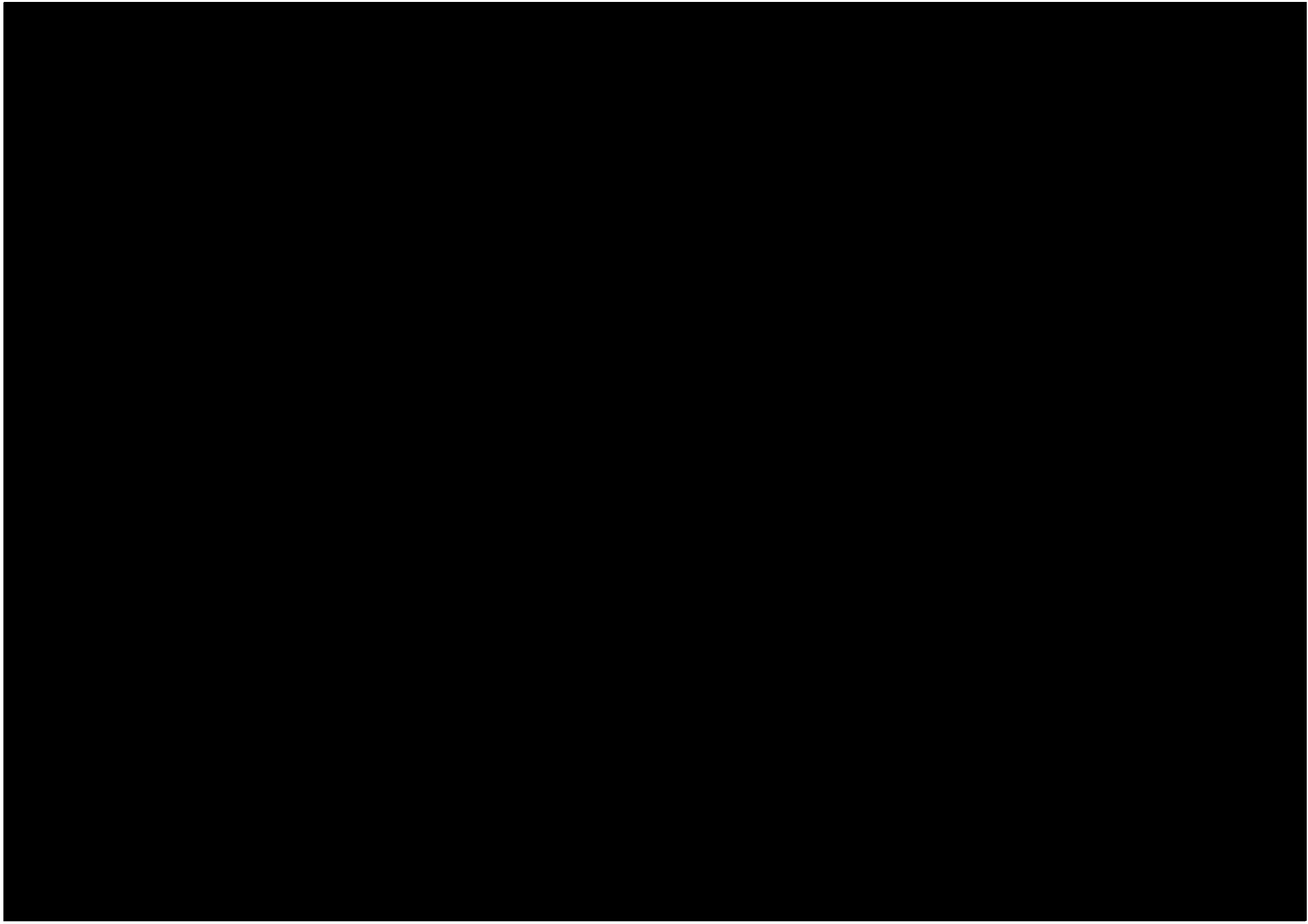


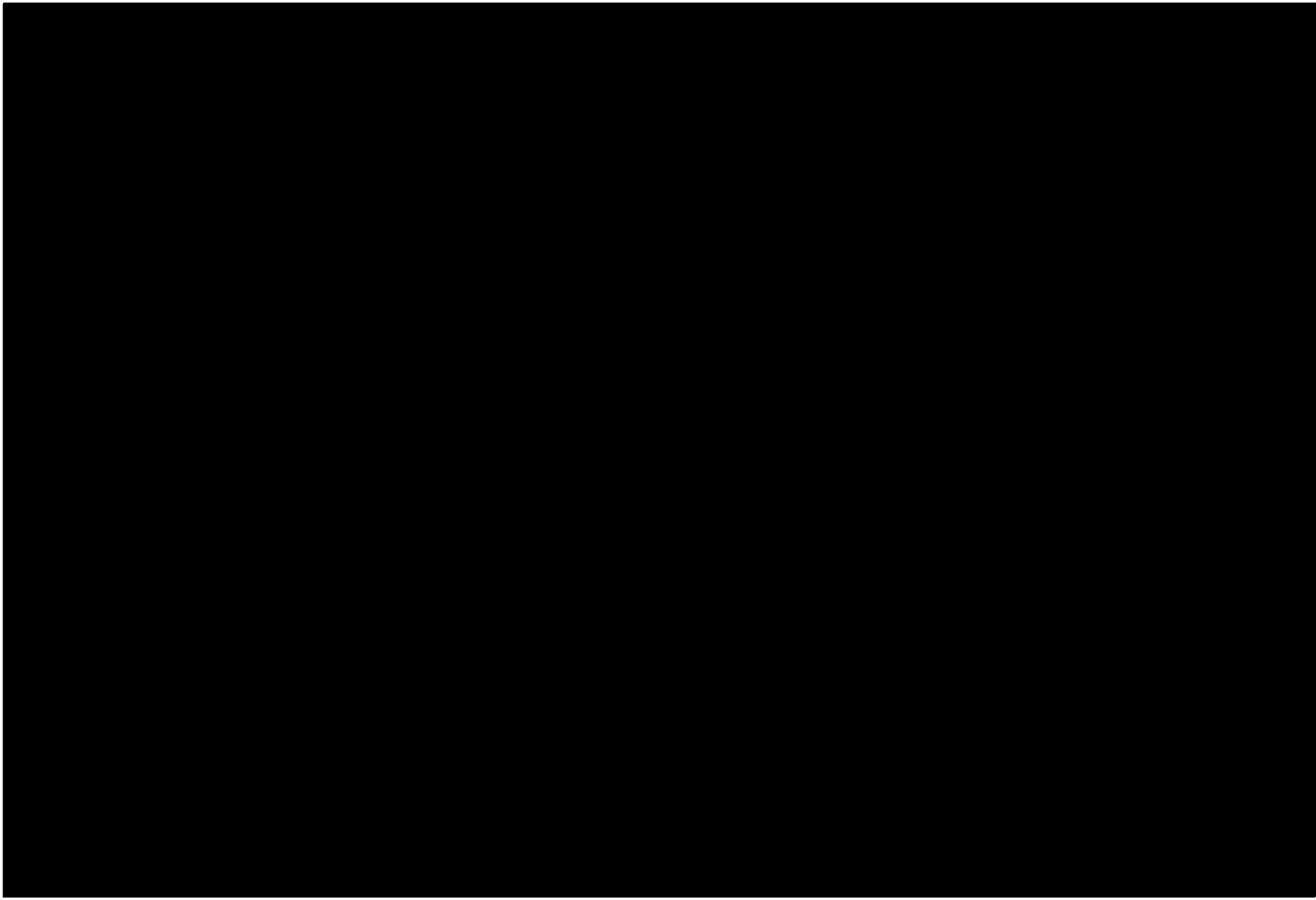


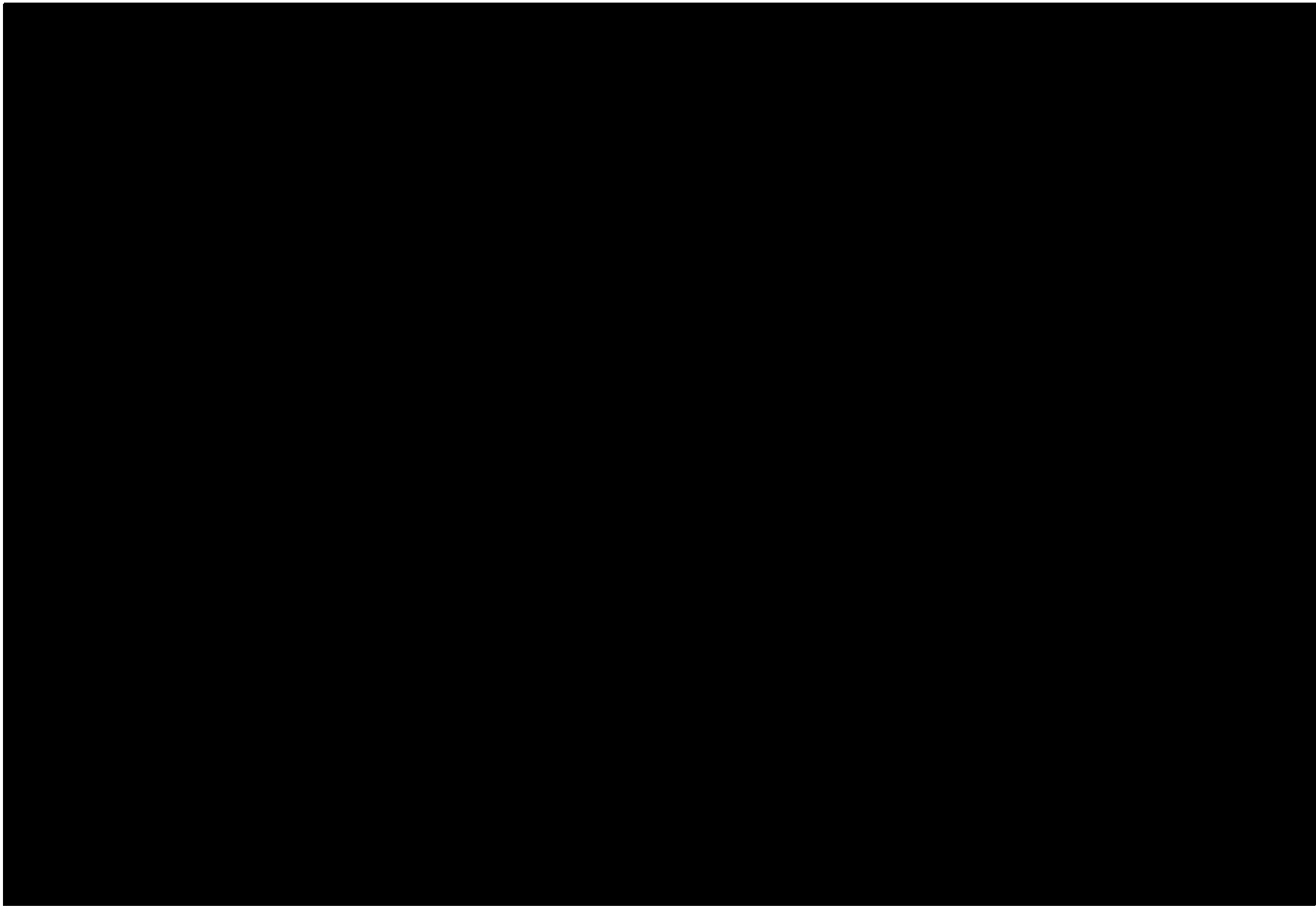


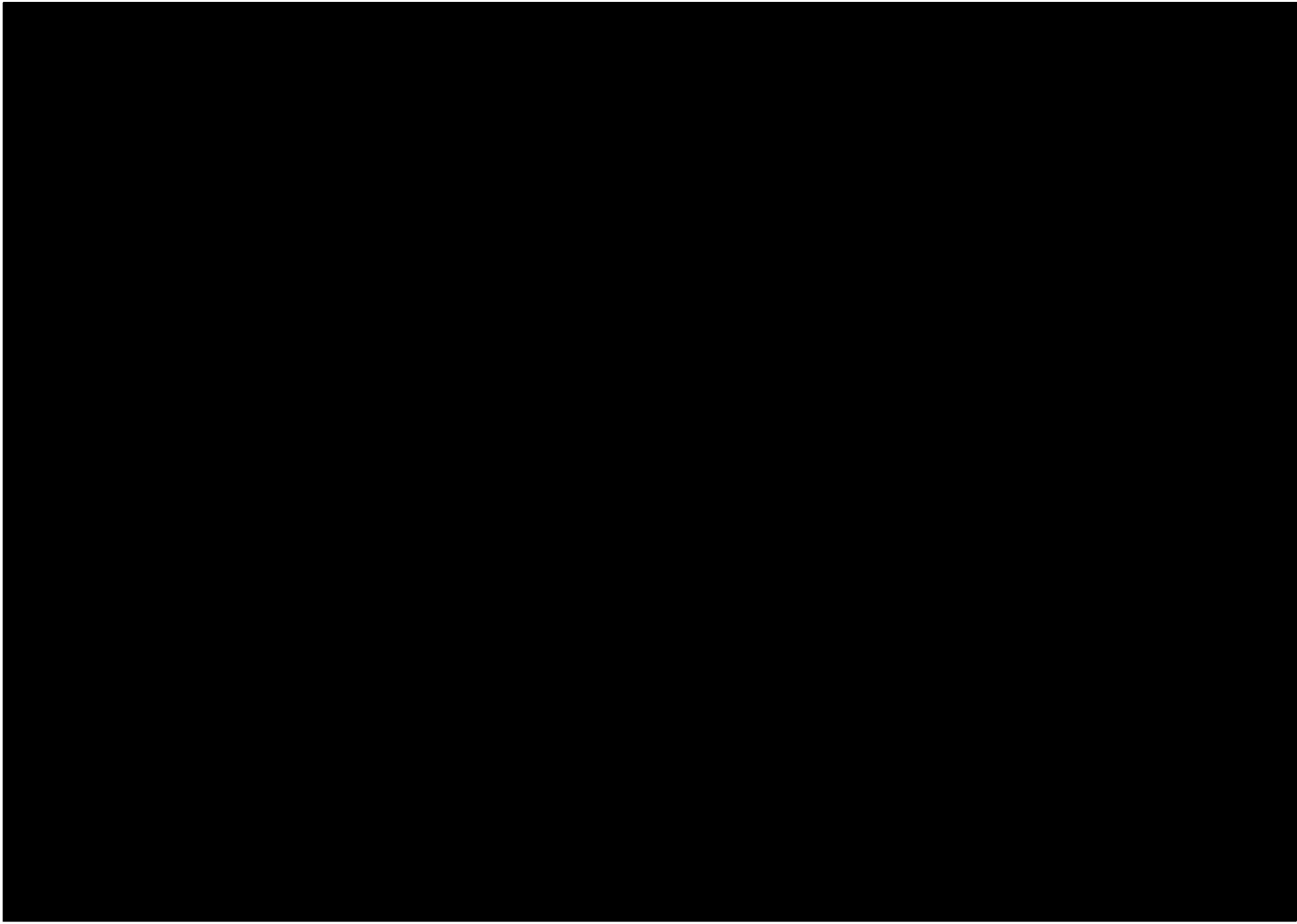


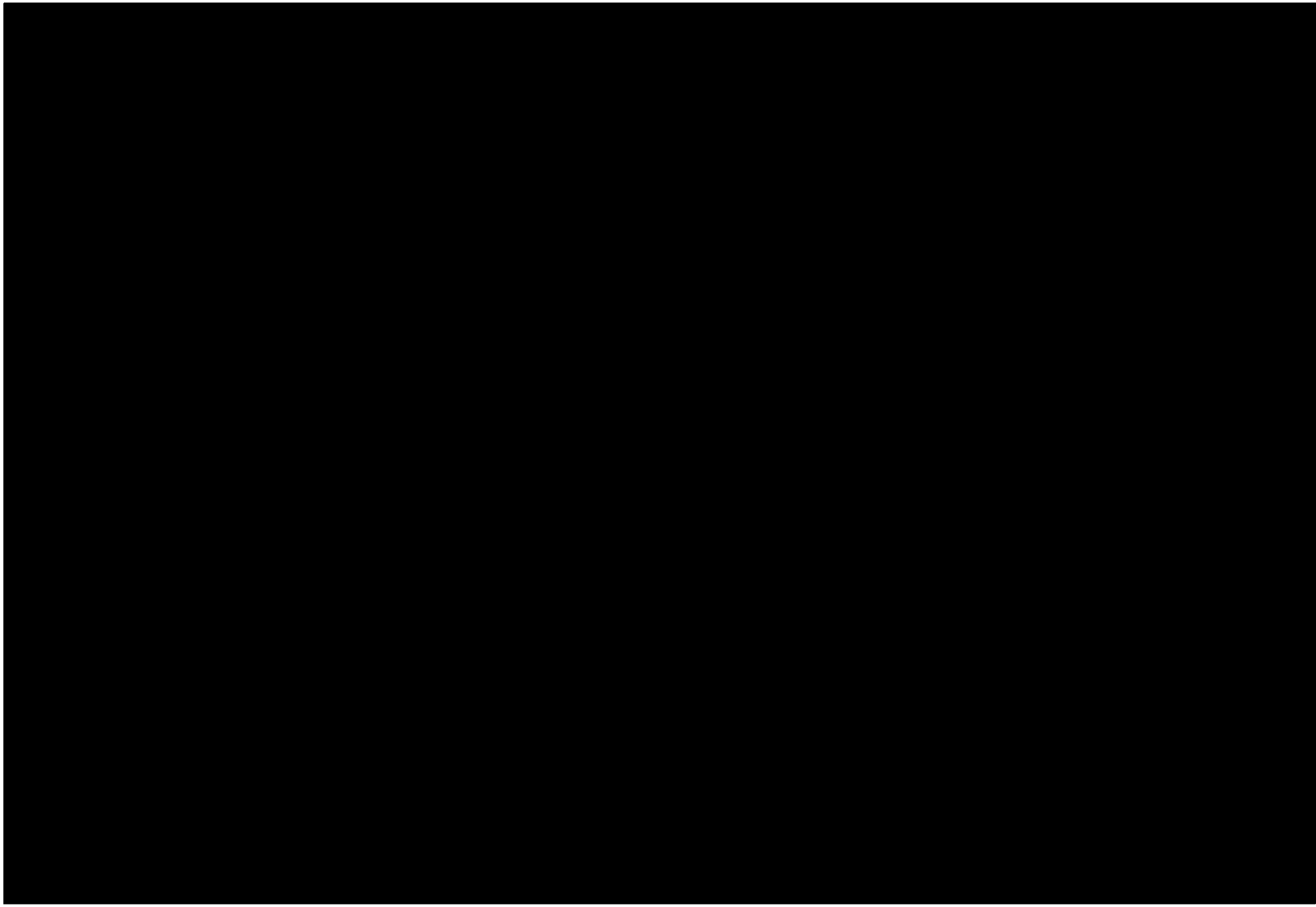


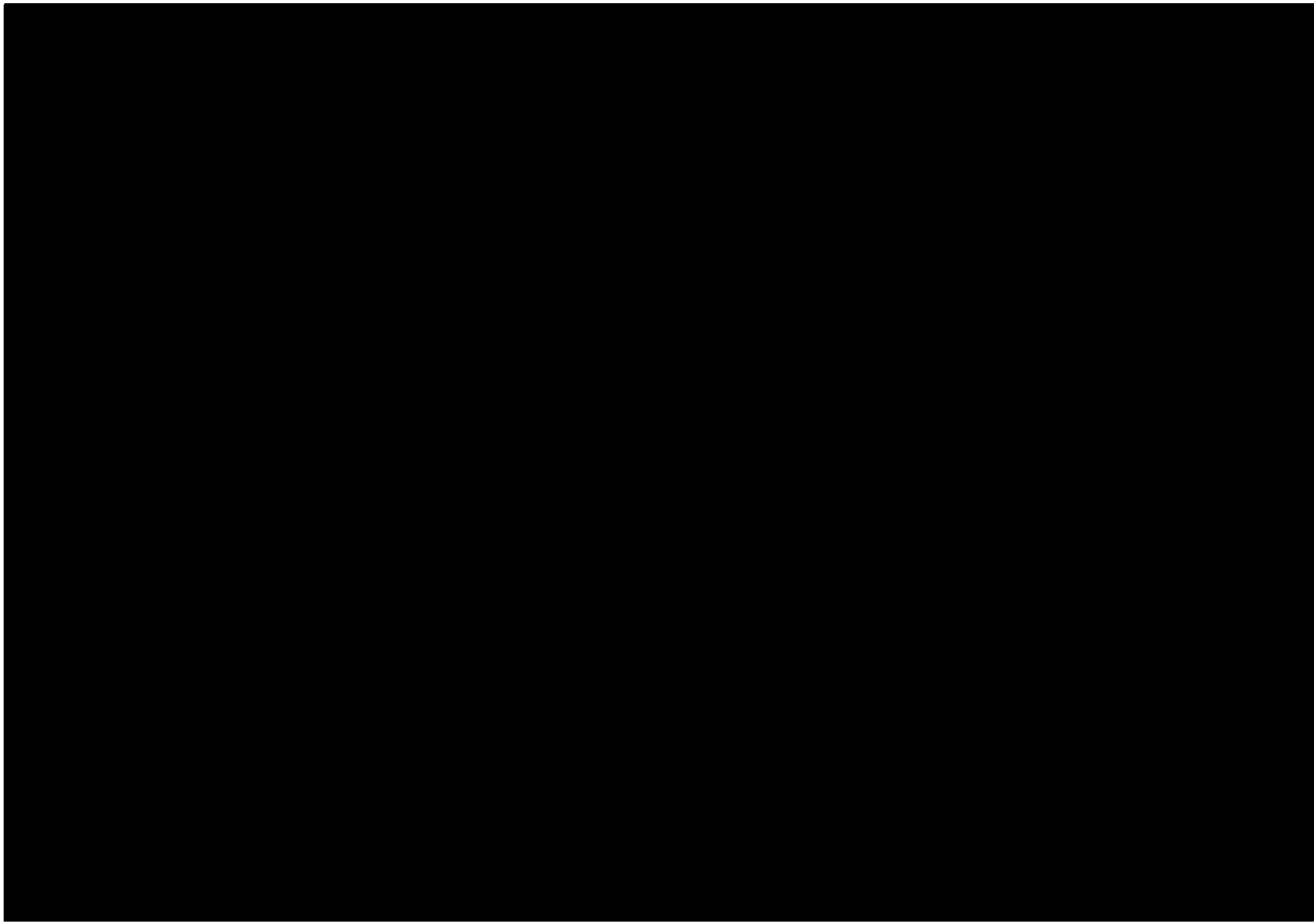












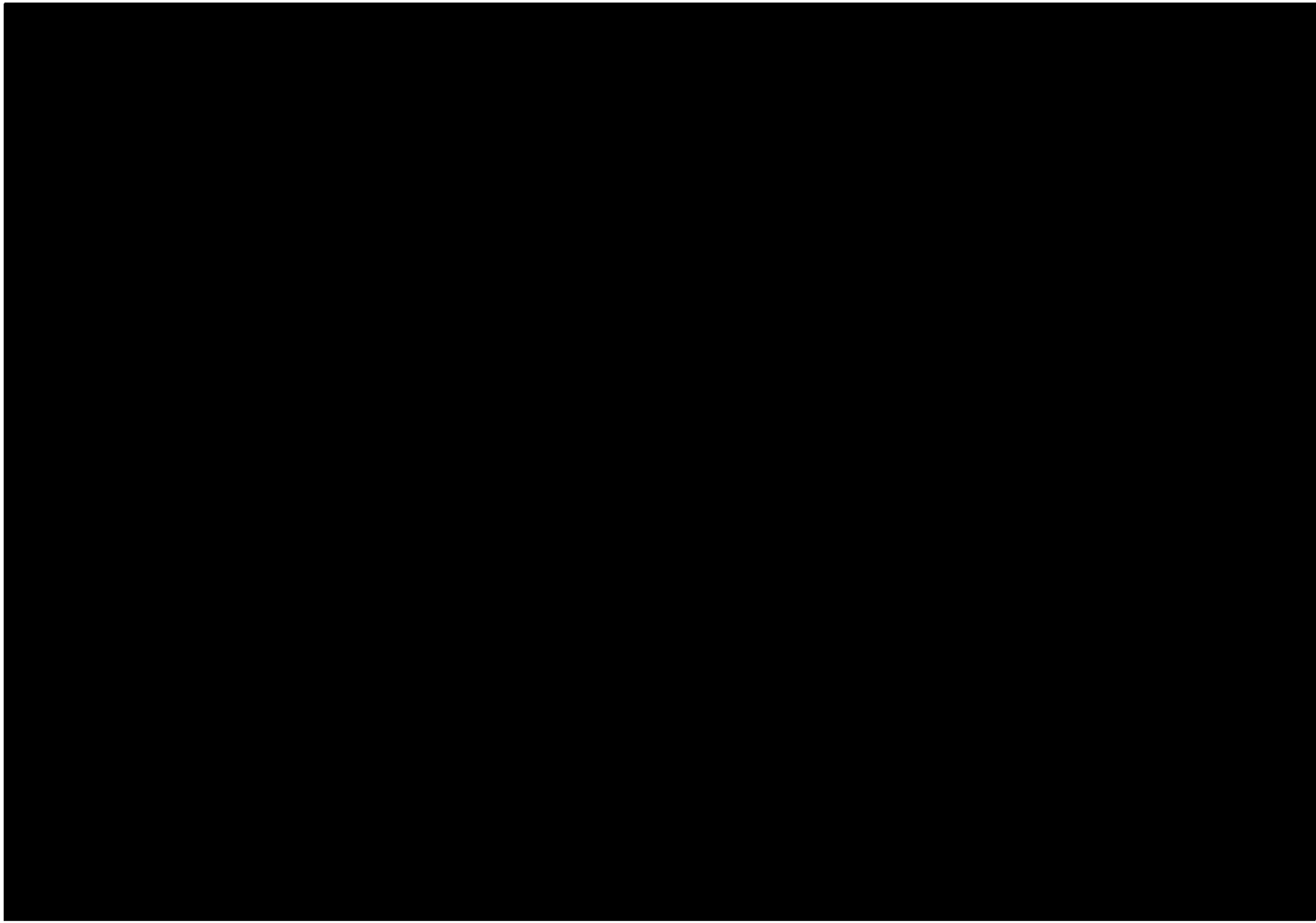
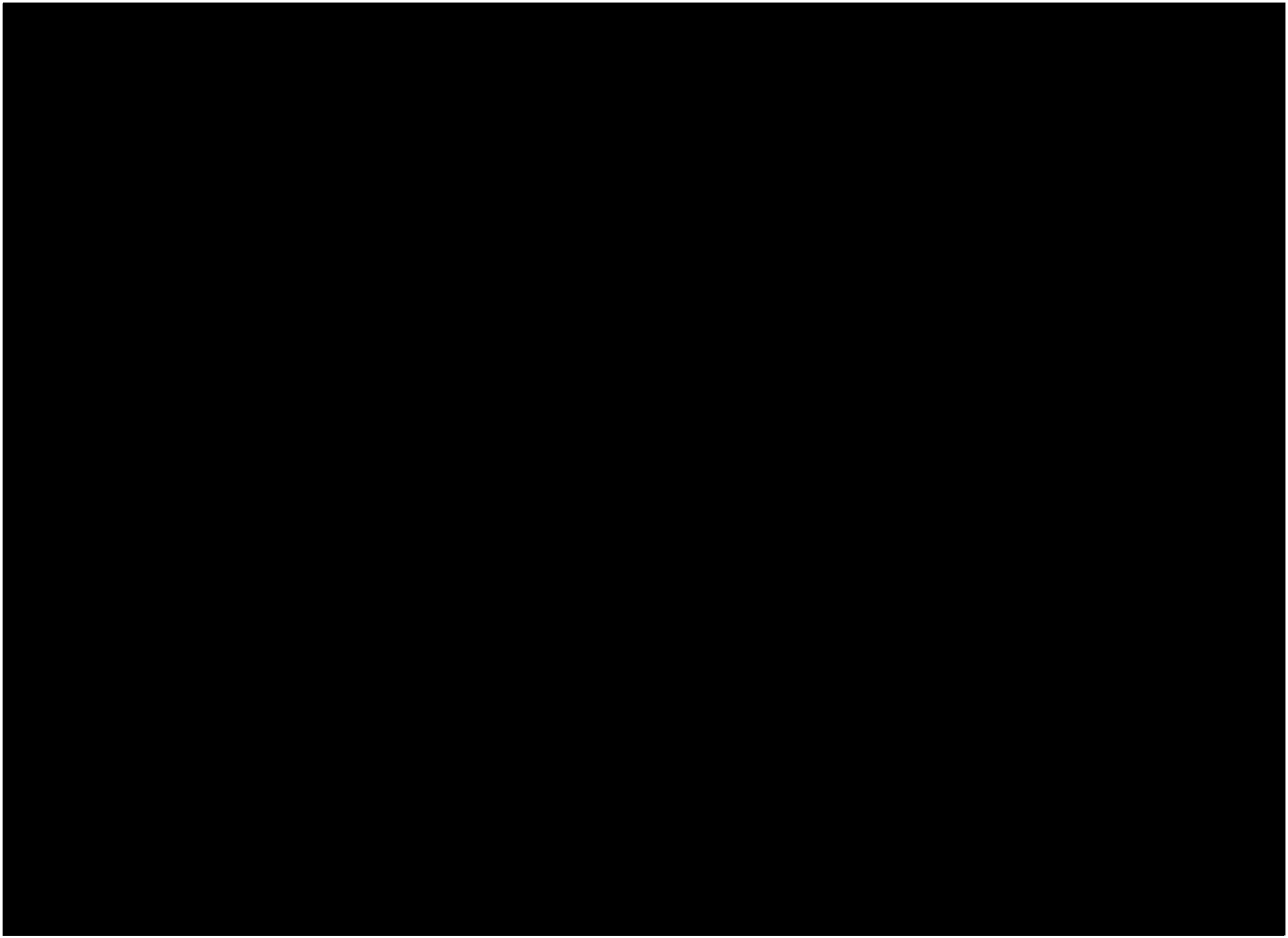
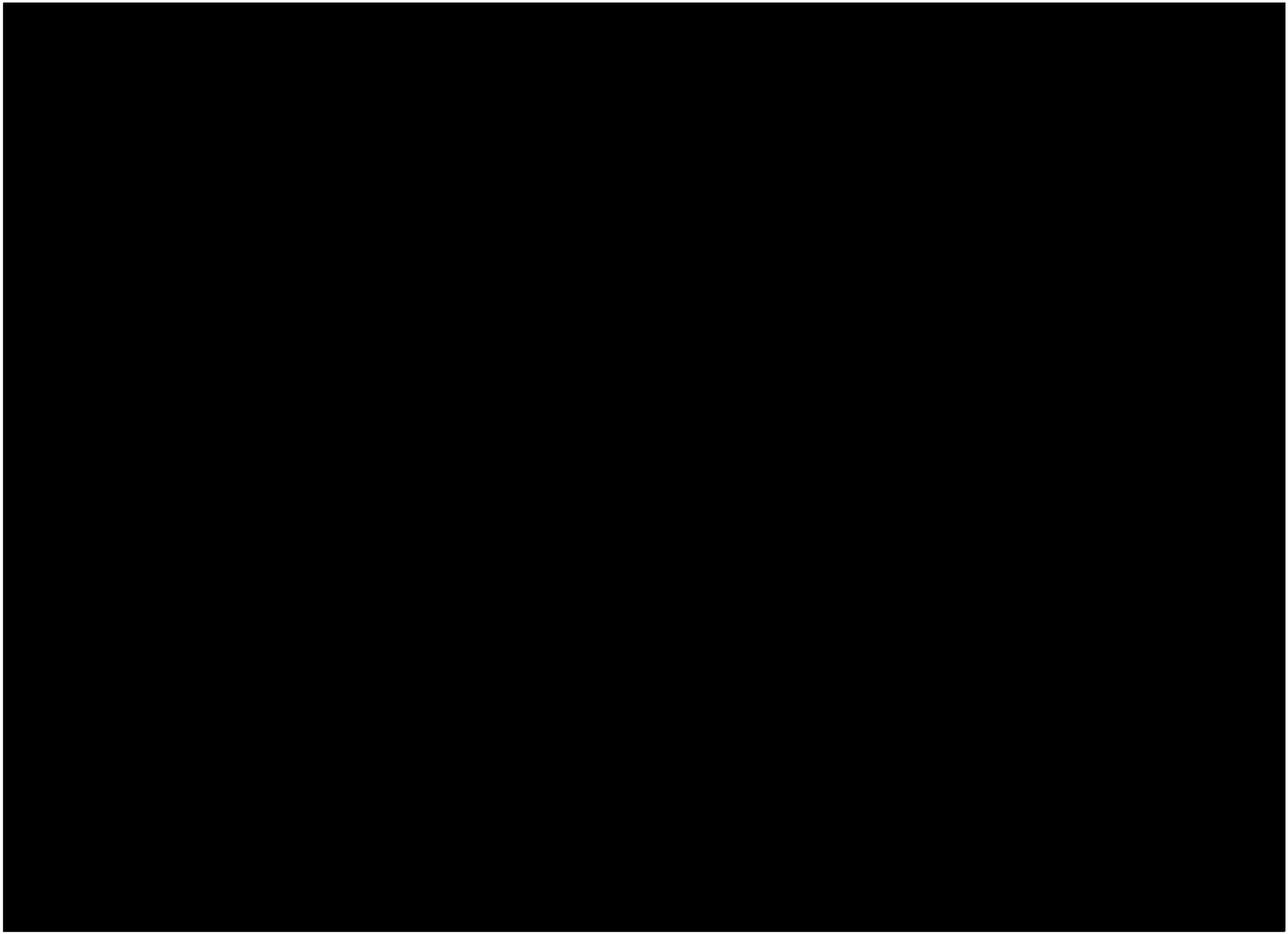


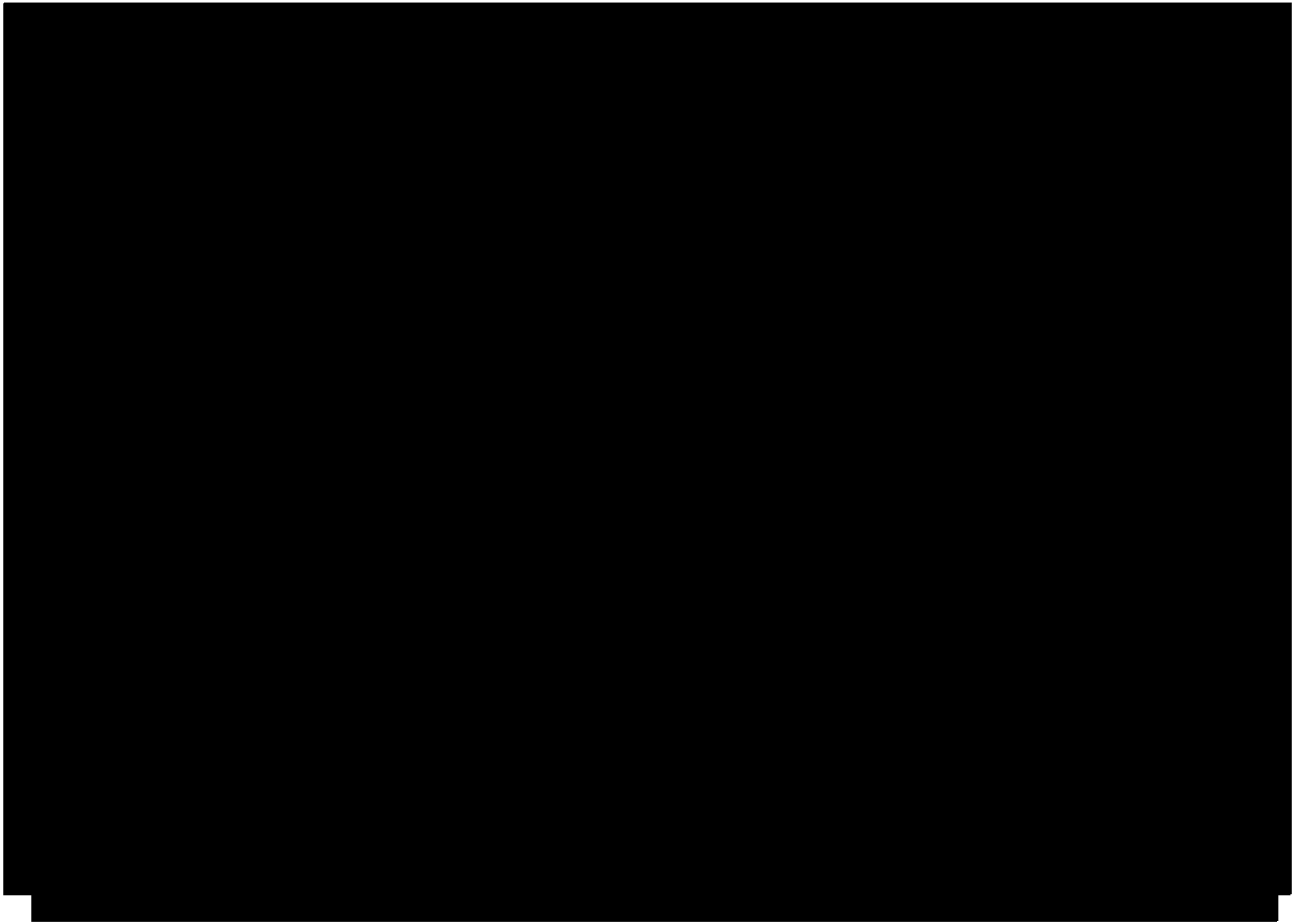
EXHIBIT G

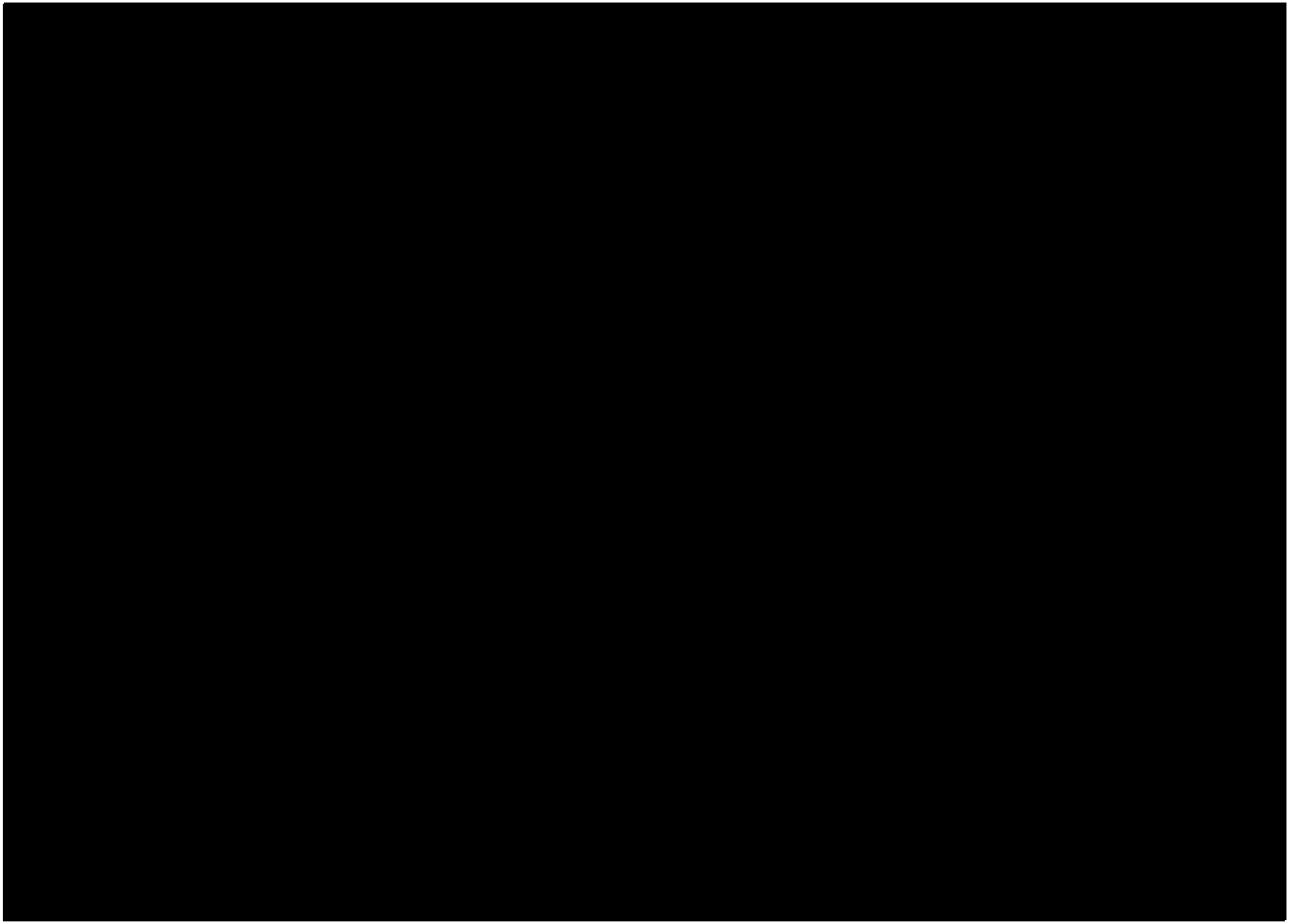
EXHIBIT 26

FILED UNDER SEAL PURSUANT TO PROTECTIVE ORDER









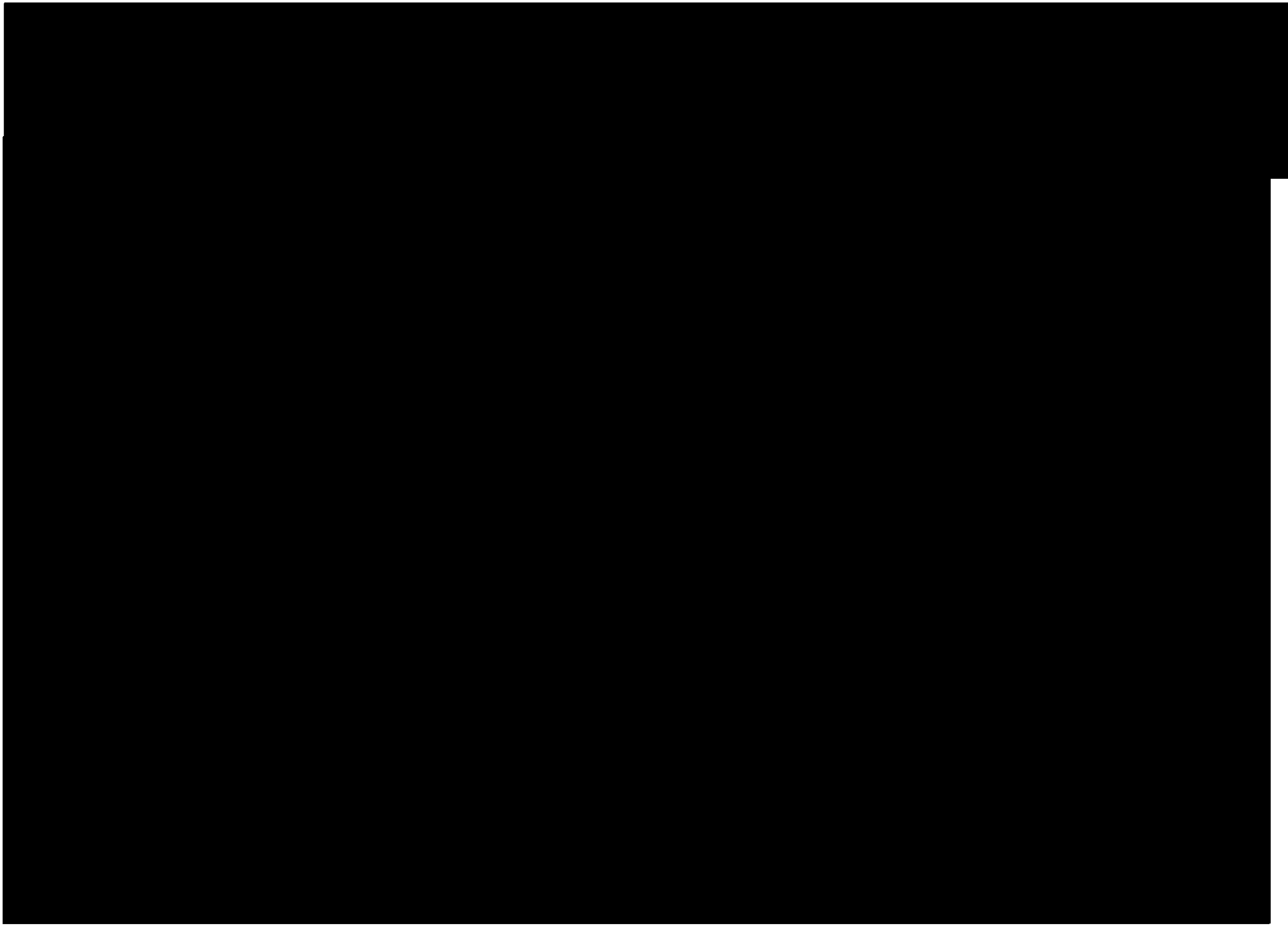


EXHIBIT H

HTTP/2

79.6k views

CDN Guide

What is the HTTP/2 Protocol

Hypertext Transfer Protocol (HTTP) is a set of standards allowing internet users to exchange website information. There have been four HTTP iterations since its introduction in 1991.

HTTP/2 was released in 2015 as a major revision to the HTTP/1.1 protocol. It was derived from the SPDY protocol as a way to improve the online experience by speeding up page loads and reducing round-trip time (RTT), especially on resource-heavy web pages.

Here we will be discussing why the new protocol was needed, its evolution from SPDY, how it differs from HTTP/1.1 and how a CDN can assist in making your site content HTTP/2 compatible.

From SPDY to HTTP/2

HTTP/1.1 was the third version of HTTP and the standard protocol for over 15 years. It introduced persistent connections for improved performance and laid the foundation for standard requests, such as GET, HEAD, PUT, and POST.

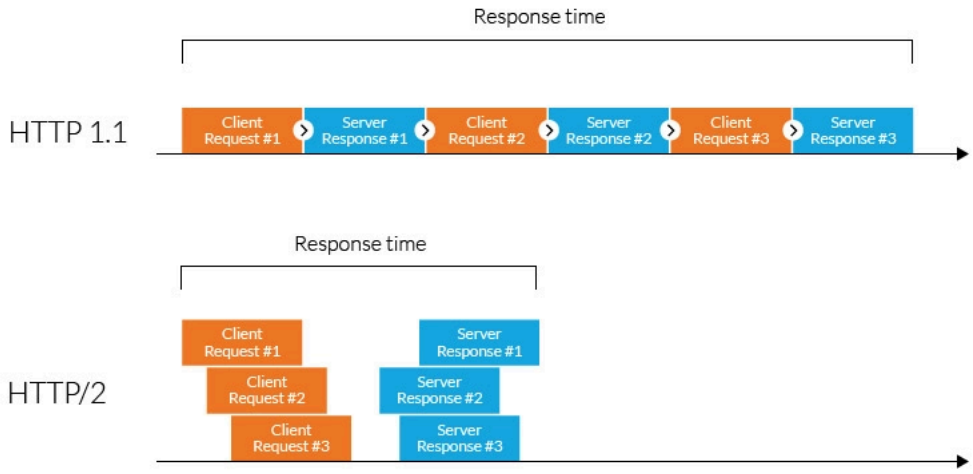
As websites became more resource-intensive, however, HTTP/1.1's limitations began to show. Specifically, its use of one outstanding request per TCP connection created significant overhead, slowing down page load times.

In 2010, Google released the SPDY protocol as a way of modifying how HTTP handles requests and responses. Its focus was on reducing latency via TCP pipelining and providing mandatory compression, amongst other features.

While HTTP/2 was initially modeled after SPDY, it was soon modified to include unique features, including a fixed header compression algorithm, (in contrast to SPDY's dynamic stream-based compression). Following its release, Google announced that it would remove support for SPDY in favor of HTTP/2.

HTTP/1.1 vs. HTTP/2 Protocol

HTTP/2 improved on HTTP/1.1 in a number of ways that allowed for speedier content delivery and improved user experience, including:



Binary protocols – Binary protocols consume less bandwidth, are more efficiently parsed and are less error-prone than the textual protocols used by HTTP/1.1. Additionally, they can better handle elements such as whitespace, capitalization and line endings.

Multiplexing – HTTP/2 is multiplexed, i.e., it can initiate multiple requests in parallel over a single TCP connection. As a result, web pages containing several elements are delivered over one TCP connection. These capabilities solve the head-of-line blocking problem in HTTP/1.1, in which a packet at the front of the line blocks others from being transmitted.

Header compression – HTTP/2 uses header compression to reduce the overhead caused by TCP's slow-start mechanism.

Server push – HTTP/2 servers push likely-to-be-used resources into a browser's cache, even before they're requested. This allows browsers to display content without additional request cycles.

Increased security – Web browsers only support HTTP/2 via encrypted connections, increasing user and application security.

HTTP/2 Implementation and CDN

Google's decision to stop supporting the SPDY protocol has made upgrading to HTTP/2 imperative for online businesses wishing to reduce RTT and speed up page load times.

Migrating to HTTP/2, however, can be complicated for a number of reasons, including:

HTTPS compatibility – The new extension to Transport Layer Security (TLS) means a site must first be HTTPS compatible to use HTTP/2.

Server upgrades – All of your servers need to be upgraded from HTTP/1.1 to HTTP/2, a potentially cumbersome and error prone process.

Bug fixes – HTTP/2 requires your developers and designers to come up with new solutions to overcome HTTP/1.1 bugs, as they can create issues with the new standard.

The Imperva CDN solves these issues by acting as an intermediary between site visitors and your origin servers. This automatically upgrades your servers from the moment you onboard our services, without the hassle of migrating to HTTP/2 on your own.

To learn more, visit our reverse proxy page.

Latest Articles

Network Security

What is a CDN

622k Views

Network Security

Cache Control

412.4k Views

Network Security

Minification

292.2k Views

Network Security

Keep Alive

216k Views

Network Security

Lazy Loading

204.3k Views

Network Security

CDN Cac

179.4k Viev

THALES
CYBERSECURITY
imperva

+1 866 926 4678

Partners

- Imperva Partner Ecosystem
- Channel Partners
- Technology Alliances
- Find a Partner
- Partner Portal Login

Resources

- Imperva Blog
- Resource Library
- Case Studies
- Learning Center

About Us

- Why Imperva
- Who We Are
- Events
- Careers
- Press & Awards
- Contact Information

Network

- Network Map
- System Status

Support

- Emergency DDoS Protection
- Support Portal
- Imperva Community
- Documentation Portal
- API Integration
- Trust Center

English

Cookies Settings

Trust Center

Modern Slavery Statement

Privacy

Legal

EXHIBIT I

(https://www.theknowledgeacademy.com/)

Excellent

What is a Session ID? Everything You Need to Know

Scarlett Adams 04 November 2025

A Session ID is a unique set of characters used to recognise and track a user's session on a website or app, transmitted via cookies, URL, or hidden form field. It helps track activities like logging in, adding items to a cart, or navigating between pages. It ensures smooth navigation, maintains login status, and secure interactions.

Training Outcomes Within Your Budget!

We ensure quality, budget-alignment, and timely delivery by our expert instructors.

Share this Resource

Table of Contents

You close your browser, come back, and the website still remembers you. Ever wondered how that happens? That smooth experience isn't some magic. The mastermind behind this functionality is the Session ID, a tiny but powerful code that helps websites recognise you.

From keeping you logged in to saving your preferences or progress, Session IDs make online journeys simple, seamless, and secure. In this blog, you can discover what a Session ID is, how it works, where it is used, and much more, all in very simple words. Continue reading!

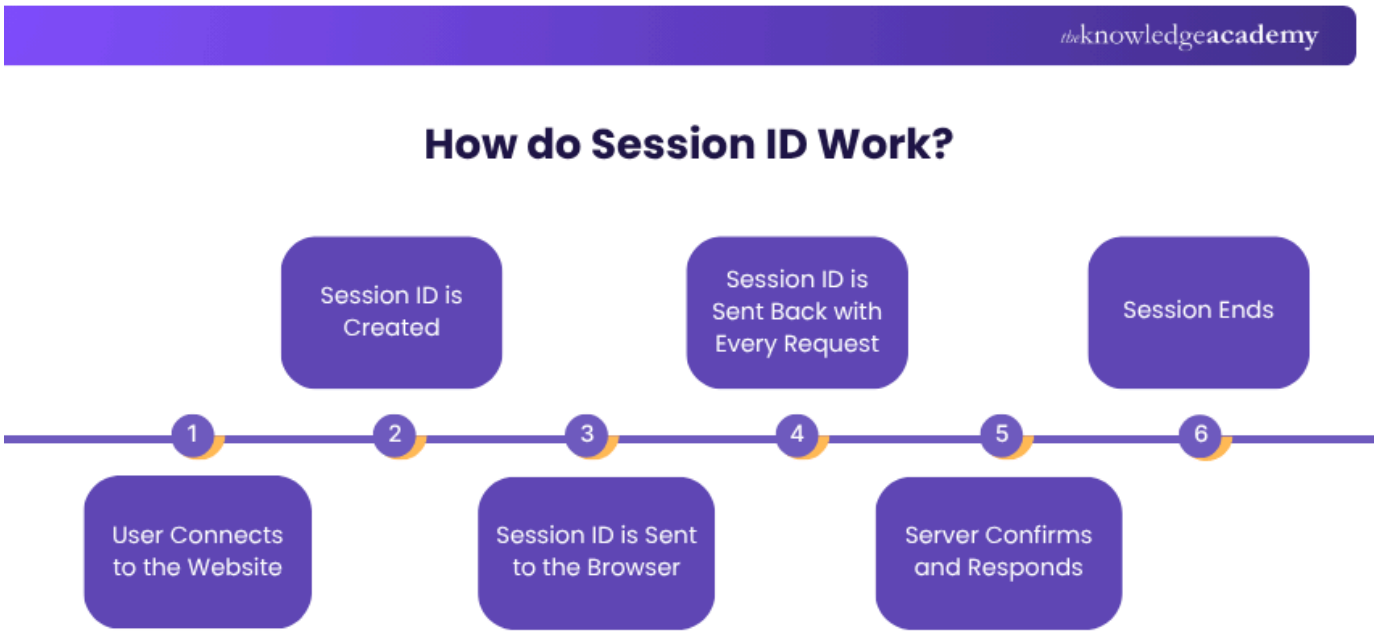
What is a Session ID?

A session ID, also known as a session token or session identifier, is a unique string of characters assigned by a web server when a user visits a website. This identifier allows the server (https://www.theknowledgeacademy.com/blog/what-is-a-server/) to recognise and remember the user throughout their visit, which is referred to as a session.

A session is a limited period of interaction between your browser (the client) and the website's server. During this time, the Session ID helps the server keep track of your actions, like staying logged in, filling out a multi-page form, or watching a video from where you left off.

How Do Session ID Work?

Session ID works by helping a website recognise and remember users during their visit. Since websites use HTTP or HTTPS, which are stateless and don't remember previous actions, Session IDs link all of a user's actions during a session. Here's how exactly it works:



1) User Connects to the Website: When a user visits a website (https://www.theknowledgeacademy.com/blog/what-is-website/), the server will create a session. This happens immediately or after the user logs in.

2) Session ID is Created: The web server generates a unique Session ID for the user. Instead of using simple numbers, it is created with complex IDs with mixed letters, numbers, and symbols.

3) Session ID is Sent to the Browser: The server sends the Session ID to the user's browser. It will be stored as a cookie. This ID identifies the user throughout the session.

4) Session ID is Sent Back with Every Request: For every new page or action, the browser sends the Session ID to the server. This allows the server to match the request with the correct session data, like login info, progress, or cart items.

5) Server Confirms and Responds: The server checks the Session ID to make sure it is valid. If it is, it completes the requested action, such as loading a page or processing a form.

6) Session Ends: The session ends when the user logs out, closes the browser, or is inactive for a while. At this point, the Session ID is invalidated, and the user must start a new session to continue.

This process ensures a secure and smooth experience across multiple pages, without re-entering your information on every request.

Where and Why are Session IDs Used?

Session IDs are widely used across many websites and apps, including:

1) E-commerce Sites: To keep track of shopping cart items or recently viewed products.

2) Banking and Finance Websites: To maintain secure access during transactions.

3) Online Learning Platforms: To track lesson progress and user login.

4) Social Media Platforms: To keep users logged in.

5) Membership Sites or Forums: To keep users signed in and manage their sessions.

Session IDs are used for various purposes. Below are important scenarios of its usage:

1) Smooth User Experience: Session IDs help users log in and track their activities across pages.

2) Enhanced Security: They ensure only the correct user can access their data. This helps to keep sessions private and protected.

3) Better Website Usability: They allow things like shopping carts and preferences to work without interruptions.

4) Anonymous Tracking: Session IDs do not store personal data but help connect actions from the same user.

Methods of Transmitting Session ID

There are three primary methods used to transmit session IDs between a browser and a server. Let's explore each of them below:

1) Cookies

Cookies are small files stored in your browser. When you visit a website, the server generates a session cookie containing your session ID. This cookie is automatically sent back to the server with every request you make, such as navigating to another page or adding an item to your shopping cart.

2) URL Parameter

If cookies are disabled in your browser, the Session ID can be added directly to the URL as a parameter. This method attaches the Session ID to the web address, like this:

https://www.example.com/page?sessionid=123abc

This lets the server recognise your session and link it to the page activity even without cookies.

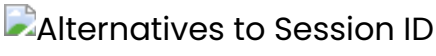
3) Hidden form Field

Another way to transmit a session ID is through a hidden form field. This is a piece of information embedded within a form that users do not see. When the form is submitted (for example, by clicking “Submit” or “Next”), the hidden field sends the session ID back to the server along with the rest of the form data.

Explore the coding basics for responsive web layouts with our **Website Design Course (https://www.theknowledgeacademy.com/courses/app-and-web-development-training/website-design-course/)** – Join soon!

What are Alternative Types to Session ID?

While Session IDs are common, other methods are also used for managing sessions, especially in more advanced applications. Here are some of the alternatives to Session IDs:


Alternatives to Session ID

1) Tokens (Such as JWT - JSON Web Tokens)

Tokens are small pieces of data stored in the user’s browser. Unlike Session IDs, which store user data on the server, tokens carry user data inside them.

Benefits:

1) Works well without server storage

2) Easily scalable

3) Can include user roles and permissions

2) Local Storage

Modern **web browsers (https://www.theknowledgeacademy.com/blog/what-is-a-web-browser/)** allow storing data in local storage. This can hold session details locally without sending them on every request.

Benefits:

1) Large storage capacity

2) Simple to use for non-sensitive information

3) Good for offline web apps

3) Cookies

Apart from Session ID cookies, persistent cookies are also used for "Remember Me" features or long-term preferences.

Benefits:

1) Easy to implement and manage

2) Can be used for personalisation

3) Reduces need for repeat logins

4) OAuth

OAuth is a secure method that allows users to log into websites using third-party accounts like Google, Facebook, or Apple.

Benefits:

1) Very secure, no need to type passwords into every website

2) Ideal for connecting with third-party services

3) Reduces password-related risks

Acquire the necessary skills for Web Development, including HTML, CSS, and JavaScript with our **Web Development Training (https://www.theknowledgeacademy.com/courses/app-and-web-developer-training/web-development-training/)** – Sign up anytime!

How Secure are Session ID?

Session IDs are powerful, but they must be managed carefully. If they're not handled carefully, they can be stolen or misused, putting users at risk. There are a few ways attackers might steal Session IDs:

1) Through public Wi-Fi without encryption

2) Using malicious scripts (like cross-site scripting or XSS)

3) By capturing Session IDs from URLs if they're not hidden or encrypted

Here are the best practices for a secure Session ID:

1) Use long, random, unguessable Session IDs

2) Use HTTPS to encrypt data during transmission

3) Set cookies as HttpOnly and Secure

4) Implement session timeout (e.g., 15 minutes of inactivity)

5) Invalidate the Session ID on logout

6) Use IP/user-agent checks to detect stolen sessions

Conclusion

Session IDs may seem small, but they play a big role in how websites work behind the scenes. From keeping you logged in to remembering your progress or activity, they help create smooth, personalised, and secure online experiences. Knowing this simple mechanism can help you browse more safely and confidently in your everyday website usage.

Learn the technologies for versatile web solutions with **App & Web Development Training (https://www.theknowledgeacademy.com/courses/app-and-web-development-training/)** – Start building your website effectively!

Frequently Asked Questions

(https://www.theknowledgeacademy.com/)

How Do I Find My Current Session ID?

How to Get Session ID from Task Manager?

What are the Other Resources and Offers Provided by The Knowledge Academy?

What is The Knowledge Pass, and How Does it Work?

What are the Related Courses and Blogs Provided by The Knowledge Academy?

Upcoming Programming & DevOps Resources **Batches & Dates**

Node.JS Course

Node.JS Course	(https://www.theknowledgeacademy.com/courses/app-and-web-development-training/node-js-developer/)

Fri 13th Mar 2026

Enquire Now

Node.JS Course	(https://www.theknowledgeacademy.com/courses/app-and-web-development-training/node-js-developer/)

Fri 19th Jun 2026

Load More

(https://www.theknowledgeacademy.com/)

Get A Quote

WHO WILL BE FUNDING THE COURSE?

My employer | I will | Not sure

* FULL NAME

* COMPANY EMAIL

me@email.com

* MOBILE

...

MESSAGE (OPTIONAL)

By submitting your details you agree to be contacted in order to respond to your enquiry

Send enquiry

The largest global training provider.

(https://www.theknowledgeacademy.com/)

(https://www.linkedin.com/company/the-knowledge-academy/) (https://twitter.com/TKA_Training) (https://en-gb.facebook.com/The.Knowledge.Academy.Ltd/) (https://www.instagram.com/the_knowledge_academy/) (https://www.youtube.com/@TheKnowledgeAcademy.) (https://www.quora.com/profile/The-Knowledge-Academy-13) (https://in.pinterest.com/TheKnowledgeAcademy/) (https://www.slideshare.net/MarketingTKA) (https://medium.com/@theknowledgeacademy)

T: 01344203999 (tel:01344203999)

E: info@theknowledgeacademy.com (mailto:info@theknowledgeacademy.com)

VAT

Bookings

(https://www.theknowledgeacademy.com/)

EXHIBIT J

What is a session ID?

IONOS editorial team
04/26/2021
7 mins

Contents

Picture the scene: you're in a giant convention center where lots of different activities are on offer. You decide to go for a specific one, get your participant badge and name tag and then go into the relevant room. For this event, you are clearly marked as being a person assigned to your chosen activity. The **convention center** is like the **server**, the individual **activity** is the **web address**, and your **name tag** is your **session ID**.

These **session IDs** allow a visitor to a website to be **clearly identifiable** during their visit to the site by way of an **electronic tag** granted by the server. Other terms for the **session ID** include **session identifier** and **session token**. In this detailed guide, we will explain how a visitor to a website is assigned a session ID and why this is useful.

Where and why are session IDs used?

A session ID is a little technological helper that allows a **user** to be **clearly identified** on a website and assigned to their session. The session ID allows access to data from the user's recent session. This data is **saved on the server** of the website in question. The ID is a string of digits and letters. For example, the following string of characters represents a 32-character session ID created with PHP:

```
<?php
session_start();
    echo "The session ID is:" . session_id();
    $sid=session_id(); //creates a variable with the session ID
?>
```

If you have your own webspace with FTP access, you can try this very easily with these three lines of code. In this example test session we got the result: "The session ID is: 84266fdbd31d4c2c6d0665f7e8380fa3"

When content is requested from the server, this tag is transferred from the server to the user and therefore creates a link to the content belonging to the latest session on the server. The user's **personal data remains anonymous** – all that is determined is that the same user is accessing the site. Without this ID, the server considers the request to be new and therefore generates a new session ID.

makes it more comfortable for the shopper and helps improve the website usability. The **temporarily** saved data from the visited websites shows what content was requested. This same method also has other important functions: using this information – i.e., the session ID – targeted **ads** can be shown (banners, pop-ups, links, etc.) that are more likely to be of interest to the user; leading to a higher response quota.

Functions of a session ID

A session ID is **generated by the server** at the beginning of a session and then **transferred to the user's browser** and saved when the user sends their request. All data linked to this session is also saved by the server in a dedicated directory on its hard drive. This is generally a temporary directory, ".../tmp". As well as the session ID, other content and data are saved here, such as user IDs and, if required by the site, the contents of a shopping basket. This file might have the following content, for example:

```
/tmp/sess_84266fdbd31d4c2c6d0665f7e8380fa3
UserID|i:1142;MyCart|a:2:{i:0;s:8:"Item_Nr01";i:1;s:8:"Item_Nr02";
```

In the next section, we will explain the two main techniques used to send a session ID to the user.

How is the session ID sent to the user and back again?

There are two different ways to send a session ID.

URIs

has been granted for the first time, this changes the URI (Uniform Resource Identifier), as the session ID is tacked onto the URI as a variable. This link can be viewed using the predefined **variable $sid** as follows:

```
<a href="https://www.yourwebsite.com/cart.php?sid=$sid">www.yourwe
```

Gives the following link in the browser:

```
https://www.yourwebsite.com/cart.php?sid=84266fdbd31d4c2c6d0665f7e
```

An alternative method is to use the session ID as a **path**:

```
<a href="https://www.yourwebsite.com/$sid/cart.php">www.yourwebsit
```

This gives you the following modified link in the browser:

```
https://www.yourwebsite.com/84266fdbd31d4c2c6d0665f7e8380fa3/cart.
```

The server is then configured in such a way that the session ID is always included in the path of the relevant user request, therefore allowing them to be **identified**.

This can also be achieved using a field in a formula by “wrapping” the generated session ID in a hidden field.

```
<input type="hidden" name="sessionId" value="$sid">
< … >
```

In this way, the session ID is sent back to the server using the defined POST parameter. The sessions belonging to the current user are therefore identified.

HTTP headers

For HTTP headers **cookies are required**. A cookie is a small text file and an extension to the **HyperText Transfer Protocol** (HTTP). These text files are **saved locally** with the user and contain the session ID. When a new request is sent to the server, the content of these **session cookies** is sent with it to the server, which temporarily saves the session ID at the same time. If the session ID in the user's cookies and the one on the server match, the request goes ahead.

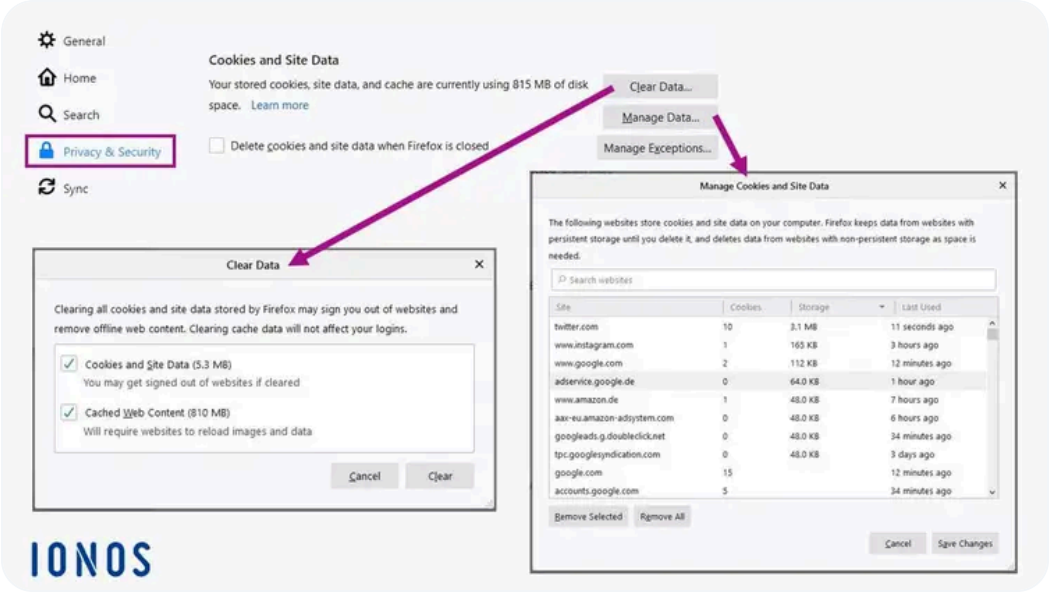
> **Note**
>
> As per the guidelines of the GDPR in Europe – as of March 2021 – a session cookie is not covered in the opt-in rules. Therefore, no active consent is required for these special cookies. However, this does **not** mean that users do not need to be informed of this.

The use of such files can be recognized, for example, if information that was once input into a form does not need to be typed again in the same field the next time the form is used. The previously entered data is suggested as soon as the first characters are typed.

How secure are session IDs?

Digital Guide

content of a session unseen, which is called session hijacking.



In the browser settings – this example uses Firefox – you can see what cookies and other data has been saved. You can manage and even delete them as you wish.

Session IDs that are sent to users and saved using **session cookies and** are **automatically deleted** when **the browser is closed**. **Closing only the relevant browser tab is not enough to do this.** Session cookies therefore do not represent a higher security risk, unlike cookies that are saved for longer periods.

Was this article helpful?

Related Products

Digital Guide

See packages

Popular Articles

What is a personal email address and how to create one

Create your personal email address with your own email domain to demonstrate...

Read more →

How do you buy a domain name? A guide

How to register and secure a domain name with the desired top-level and second-level...

Read more →

Digital Guide

What are the different types of domain endings? And what's the difference between...

Read more →

What is prompt engineering and how does it work?

What is prompt engineering and how can it be used to improve the results of ChatGPT and...

Read more →

Which website type should you choose? The 7 most popular kinds

Choosing the right website type is crucial for the success of any online project....

Read more →

Related articles

Digital Guide

Log analysis: What the web server log reveals about your visitors

How many pages are accessed by a single user when they're visiting your website? And which links or search queries did they use to lead them to you? To answer such questions, well-...

Data Analysis **Advice**

Read more →

About IONOS

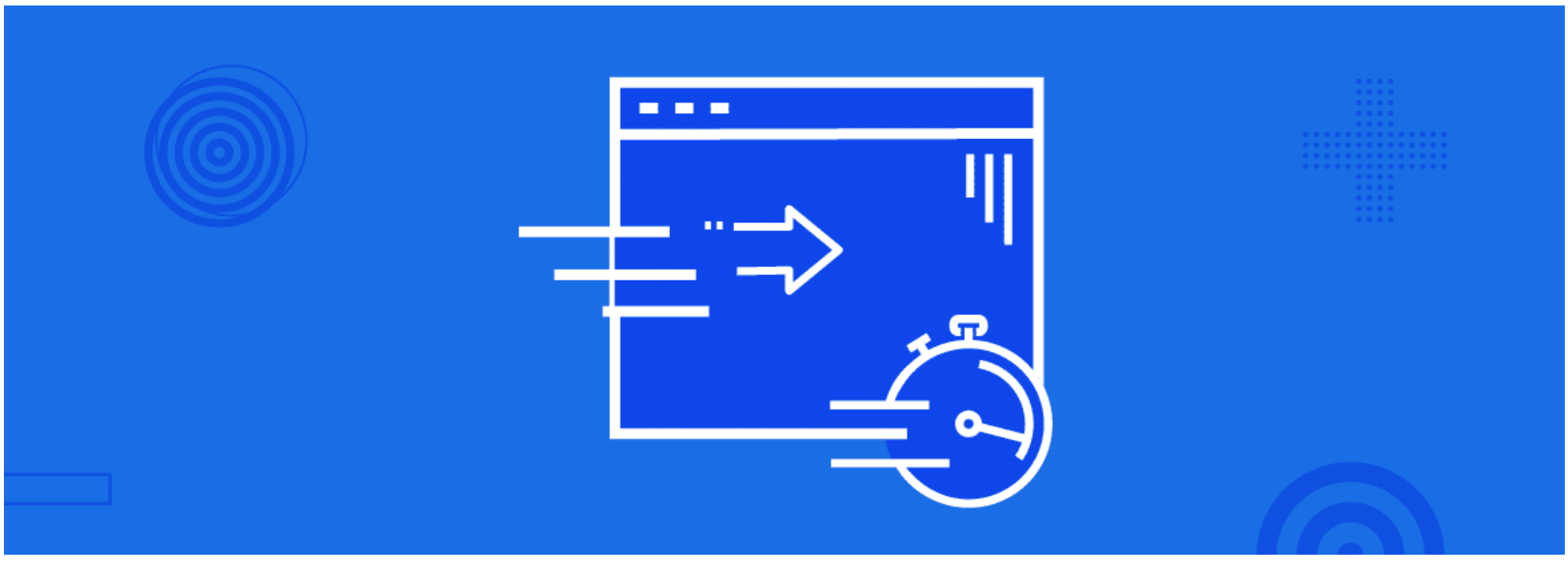
Digital Guide

Your digital partner

EXHIBIT K

Session Management: An Overview

April 29th, 2021



Session management manages sessions between the web application and the users. The communication between a web browser and a website is usually done over HTTP or HTTPS. When a user visits a website, a session is made containing multiple requests and responses over HTTP.

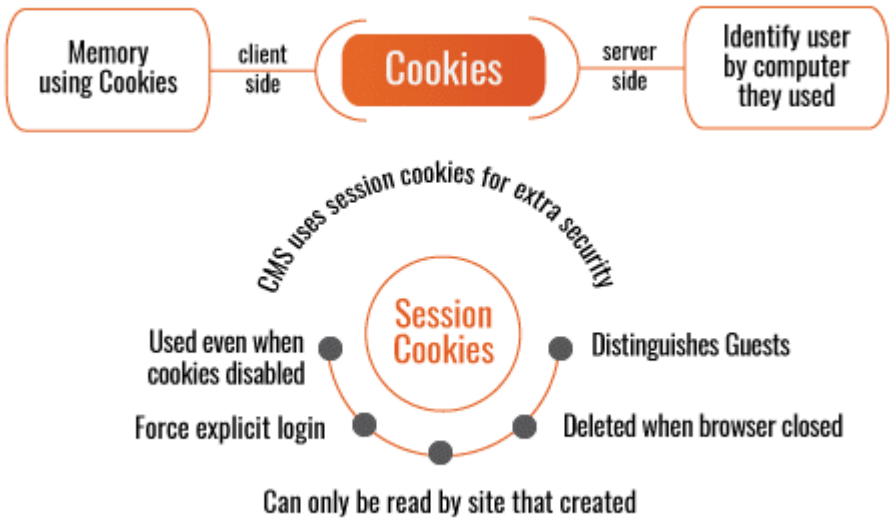
According to RFC (section 5, RFC2616), HTTP is a stateless protocol. In this process, each request and response is independent of other web processes. Session management capabilities linked to authentication, access, control, and authorization are commonly available in a web application.

Source: OWASP

Modern web applications require maintaining multiple sessions of different users over a time frame in case of numerous requests. Regarding security, session management relates to securing and managing multiple users' sessions against their request. In most cases, a session is initiated when a user supplies an authentication such as a password. A web application makes use of a session after a user has supplied the authentication key or password. Based on the authentication, the user is then provisioned to access specific resources on the application.

Session ID

A session ID, also known as a session token, is a unique number ID assigned by a website server to a specific user for the duration the user is on the website. This session ID's storage is in the form of a cookie, form field, or URL. Each time a user opens a web browser and visits a website, a session ID is generated. The session ID remains the same for some time. If a user closes the browser and reopens the web browser to visit a site, a new session ID is created again.
The token or session ID binds the user's credentials for authentication for user HTTP traffic. The web application then applies the access control and permissions.



Source: Composr

Attacks related to Sessions

When authentication and session management are not properly secured and configured, adversaries can steal the passwords or session IDs to access user's accounts and spoof their IDs. If the session IDs are compromised, adversaries can impersonate other users on the network, system, or application. This kind of attack is known as session hijacking, where the hacker can use brute force, predict and expose the session tokens.
Session fixation is another type of attack that enables attackers to hijack a user's valid session ID.

Source: Security Boulevard

According to Acunetix, "The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application. When authenticating a user, it doesn't assign a new session ID, making it possible to use an existent session ID. The attack consists of inducing a user to authenticate himself with a known session ID and then hijacking the user-validated session with the knowledge of the used session ID. The attacker has to provide a legitimate web application session ID and try to make the victim's browser use it."

Best Practices for Implementing Session Management

Having many points of attack related to a web session or a large attack surface can compromise web applications and sessions in

Avoid sending sensitive traffic over unencrypted channels, i.e. HTTP. Setup the secure flag, which will ensure that data is transmitted over encrypted protocols such as HTTPS. The HTTP flag should only be set on session cookies to prevent session hijacking, which can be caused due to client-side javascript execution.

- Generation of new session cookies

New session token generation should be ensured at every step of the authentication and interaction process, i.e. when a user visits an application or website and when the user gets authenticated. Apart from this, a new session should be created when a user exits from the application. Cookies should have an expiration time. In this way, if an account is inactive for a long time the session will expire.

- Session cookies configuration

Session tokens should not be easily guessable, they should be long, unique and unpredictable. Doing so will decrease the chances of an attacker being successful in using brute force to figure out the session token. The expiration time of persistent cookies should be no longer than 30 minutes, so that attacks such as session fixation can be prevented.

Session Management Best practices according to OWASP

The following are some of the best practices as per the OWASP

- Use a trusted server for creating session identifiers.
- Efficient algorithms should be used by the session management controls to ensure the random generation of session identifiers.
- Ensure that the logging out functionality terminates the associated connection/session entirely.
- Ensure that session inactivity timeout is as short as possible, it is recommended that the timeout of the session activity should be less than several hours.
- Generate a new session identifier when a user re-authenticates or opens a new browser session.
- Implement periodic termination of sessions, especially for applications that provide critical services.
- Appropriate access controls should be implemented to protect all server-side session data from unauthorized access by other users.

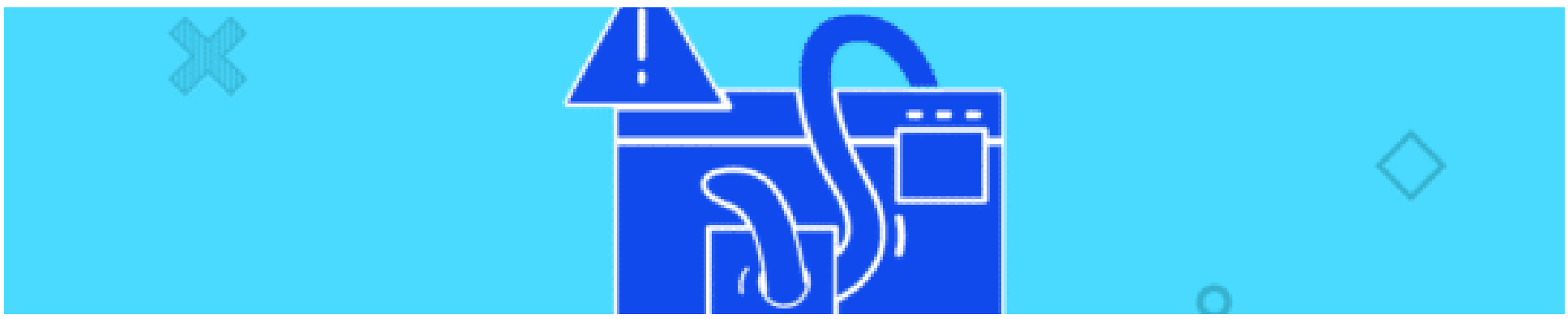
Conclusion

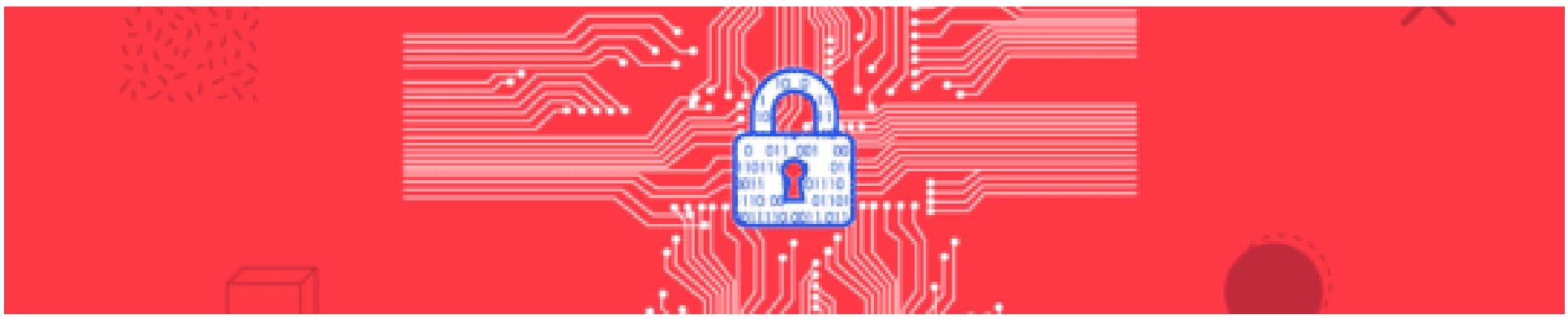
Session management control and implementation should be taken seriously by organizations that provide critical services locally or globally. Software developers should implement best practices for all session management to evade threats and attacks that can compromise the confidentiality, integrity and availability of their applications and web services.

Recommended content

Ruby Malware and Prevention Methodology

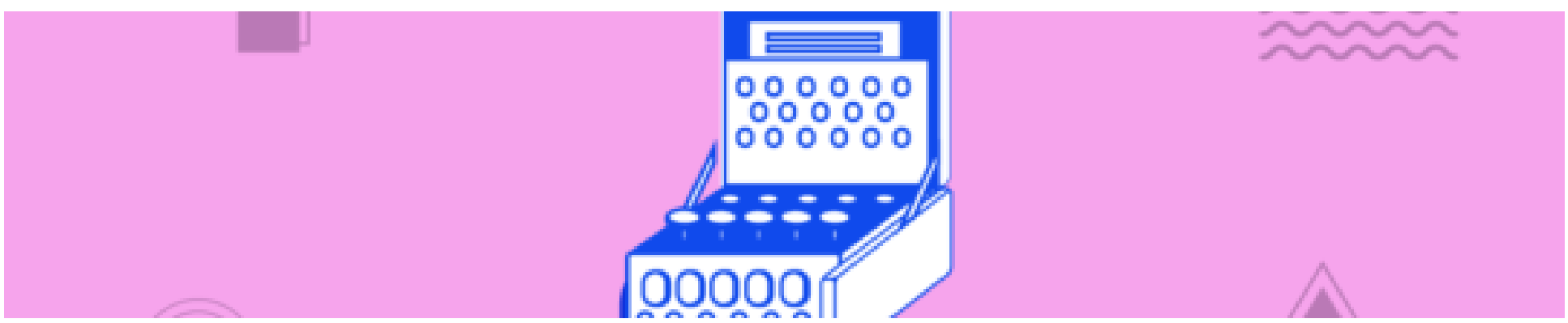
Tuesday June 28, 2022





How to Automate Server Hardening

Wednesday June 15, 2022



What is the Diffie-Hellman Key Exchange and How Does it Work?

Wednesday June 8, 2022

RESOURCES

Blog

Webinar

Events

SECURE CODING

About Us

Contact Us

Privacy Policy

NEWSLETTER

Enter your email address

SUBSCRIBE

I agree to receive email updates from Secure Coding

EXHIBIT L

```sql
-- Squarespace-wound discarded returns

SELECT
    ds,
    entity,

    /* ---------- TOTAL ---------- */
    COUNT(*) AS total_events,

    /* ---------- USED IN PROD ---------- */
    COUNT(CASE WHEN [redacted] = 'used_in_prod' THEN 1 END) AS
    used_in_prod_events,
    ROUND(100.0 * COUNT(CASE WHEN [redacted] = 'used_in_prod' THEN 1 END) / COUNT
    (*), 2) AS pct_used_in_prod,

    /* ---------- DISCARDED TOTAL ---------- */
    COUNT(CASE WHEN[redacted] = 'discarded' THEN 1 END) AS [redacted]
    ROUND(100.0 * COUNT(CASE WHEN [redacted] = 'discarded' THEN 1 END) / COUNT
    (*), 2) AS pct_discarded,

    /* ---------- DISCARDED: BOT ---------- */
    COUNT(CASE WHEN [redacted] = 'discarded' AND [redacted] = 'bot_traffic'
     THEN 1 END) AS [redacted],
    ROUND(100.0 * COUNT(CASE WHEN p[redacted] = 'discarded' AND [redacted]
     'bot_traffic' THEN 1 END) / COUNT(*), 2) AS pct_discarded_bot,

FROM meta.offsite_signals
  WHERE entity IN ('hrblock', 'taxact')
GROUP BY ds, entity
ORDER BY entity, ds;
```

EXHIBIT M

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: META Pixel HEALTHCARE LITIGATION	)
This document relates to: Case 3:22-cv-3580-WHO(Doe)	) NO. 3:22-cv-3580-WHO

VIDEO-RECORDED DEPOSITION
UPON ORAL EXAMINATION OF
ABHINAV ANAND

9:04 A.M.
APRIL 1, 2025
LOCATION: BELLEVUE, WASHINGTON

** ATTORNEYS' EYES ONLY **

REPORTED BY: VICKY L. PINSON, RPR-CCR Washington 2559
California No. 9845; Oregon No. 16-0442

A P P E A R A N C E S

FOR THE PLAINTIFFS:

JAY BARNES
Simmons Ha Conroy
112 Madison Avenue
New York, NY 10016-7416
212.784.6400
jaybarnes@simmonsfirm.com
ERIC S. JOHNSON
Simmons Ha Conroy
One Court Street
Alton, IL 62002
618.259.6275
ejohnsonsimmonsfirm.com

RYAN TACK-HOOPER
Terrell Marshall Law Group, PLLC
936 N. 34th Street, Ste 300
Seattle, WA 98103
206.816.6603
Ryan@terrellmarshall.com

FOR THE DEFENDANT:

ELIZABETH K. McCLOSKEY
Gibson Dunn
One Embarcadero Center, Ste 2600
San Francisco, CA 94111
415.393.4622
Emccloskey@gibsondunn.com
MATT BUONGIORNO
Gibson Dunn
2001 Ross Avenue, Ste 2100
Dallas, TX 75201
214.698.3204
Mbuongiorno@gibsondunn.com

VERONICA NAUTS - Meta counsel

VIDEOGRAPHER:
MICHAEL HEHENKAMP, Video Specialist

I N D E X
(CONFIDENTIAL ATTORNEY EYES ONLY)

I N D E X (continuing)
(CONFIDENTIAL - ATTORNEYS' EYES ONLY)

I N D E X (continuing)

(CONFIDENTIAL - ATTORNEYS' EYES ONLY)

*Exhibits 196, 197, and 198 retained by counsel

well?

MS. MCCLOSKEY: Object to form.

A. Yes. That's correct.

Q. And then but for health, because it was a restricted source, that which made it through the filter would go downstream into these five systems. Is that correct?

A. So my understanding is that between the second green box and the Deduplication, we had few other boxes doing the signals processing path which looped into processing of the data. And the drop event decision box are looking at the combined outcome of what all different processing components said about the event. If any of them said drop, it would eventually drop it.

Q. What were the other processing components that would drop an event?

MS. MCCLOSKEY: Object to form. Vague and ambiguous. Calls for speculation.

A. I recall one box about blocking on apps. There were more, but -- I recall, yeah, more which is identifying bought traffic. And then dropping data based on that.

Q. At a high level, how did Meta identify bought traffic?

MS. MCCLOSKEY: Object to form. Calls for

No. 12. We are back on the record at 7:20 p.m.

MS. MCCLOSKEY: I have no questions for the witness. We will designate this transcript AEO until we dedesignate.

MR. BARNES: Understood. Obviously I have no followup.

MS. McCLOSKEY: Okay, great. Thank you very much, Mr. Anand.

MR. BARNES: Thank you, Mr. Anand.

THE VIDEOGRAPHER: Here marks the end of the deposition of Abhinav Anand. We are going off the record at 7:20 p.m. Thank you.

(Deposition concluded at 7:20 p.m.)

(Signature was reserved.)

* * *

CORRECTION & SIGNATURE PAGE

IN RE: META PIXEL HEALTHCARE LITIGATION
UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION NO. 3:22-cv-3580-WHO
ABHINAV ANAND; TAKEN APRIL 1, 2025
REPORTED BY: VICKY L. PINSON, RPR-CCR

I, ABHINAV ANAND, have read the within transcript taken April 1, 2025, and the same is true and accurate except for any changes and/or corrections, if any, as follows:

PAGE/LINE	CORRECTION	REASON
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Signed at _____, Washington, on this date: _____.

_____
ABHINAV ANAND

REPORTER'S CERTIFICATE

I VICKY L. PINSON, RPR-CCR, the undersigned Certified Court Reporter, authorized to administer oaths and affirmations in and for the states of Washington, Oregon and California, do hereby certify:

That the sworn testimony and/or proceedings, a transcript of which is attached, was given before me at the time and place stated therein; that the witness was duly sworn or affirmed to testify to the truth; that the testimony and/or proceedings were stenographically recorded by me and transcribed under my supervision.

That the foregoing transcript contains a full, true, and accurate record of all the testimony and/or proceedings occurring at the time and place stated in the transcript; that a review of which was requested.

That I am in no way related to any party to the matter, nor to any counsel, nor do I have any financial interest in the event of the cause.

WITNESS MY HAND this 14th day of April, 2025.

_____

VICKY L. PINSON, RPR-CCR
Washington Certified Court Reporter, No. 2559
Oregon State Certified Court Reporter, No. 16-0442
California State Certified Court Reporter, No. 9845.

Elizabeth McCloskey, Esquire
emccloskey@gibsondunn.com

April 14, 2025

RE: In Re: Meta Pixel Healthcare Litigation v.
4/1/2025, Abhinav Anand (#7224247)

The above-referenced transcript is available for review.

Within the applicable timeframe, the witness should read the testimony to verify its accuracy. If there are any changes, the witness should note those with the reason, on the attached Errata Sheet.

The witness should sign the Acknowledgment of Deponent and Errata and return to the deposing attorney. Copies should be sent to all counsel, and to Veritext at cs-midatlantic@veritext.com

Return completed errata within 30 days from receipt of testimony.

If the witness fails to do so within the time allotted, the transcript may be used as if signed.

Yours,
Veritext Legal Solutions

EXHIBIT N

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

IN RE META PIXEL HEALTHCARE LITIGATION

Case No. 22-cv-03580

ERRATA SHEET FOR THE TRANSCRIPT OF THE APRIL 1, 2025, DEPOSITION OF ABHINAV ANAND

Page(s)	Line(s)	Change	Reason
8	17	**From**: And the o thing I ask is we not break in **To**: And the only thing I ask is we not break in	Typographical
11	4	**From:** Convergence API, Offline Convergence **To:** Conversions API, Offline Conversions	Typographical
12	13, 14	**From**: Convergence API **To**: Conversions API	Typographical
16	24	**From**: What do you mean by an o channel end point? **To**: What do you mean by an only channel endpoint?	Typographical
18	4	**From:** fit **To:** fed	Typographical
19	8	**From**: tables for all the Pixel data. **To**: tables for the Pixel data.	Mistranscription
19	20	**From:** Signalling the 50 ad or source classification system **To:** using the old source classification system	Mistranscription
22	20	**From**: real data on its inter-Meta system. **To**: real data when it's in to the Meta system.	Mistranscription
24	5	**From:** assist **To:** assess	Mistranscription
25	18	**From:** traded to **To:** attempted to	Mistranscription
25	19	**From:** traded to **To:** attempted to	Mistranscription
27	4	**From:** health, but health was . . . **To:** prohibited, but health was . . .	Mistranscription
27	15	**From:** teammates were working on a defined what . . . **To:** teammates were working on identifying what . . .	Mistranscription

Page(s)	Line(s)	Change	Reason
95	8	**From:** The row items in Off-Site Signals after the **To:** The row items in Off-Site Signals were after the	Mistranscription
96	2	**From:** operated at different times, there are different, like, **To:** operated at different times, there are different, like, RegEx like I said, had	Mistranscription
96	15	**From:** down to Signals Integrity. **To:** down to Signals Integrity which we just talked about that box.	Mistranscription
97	4	**From:** the deduplicated on certain rules. **To:** to remove the duplicated data based on certain rules.	Mistranscription
97	12	**From:** Drop event was a staging Meta Signals **To:** Drop event was a stage in Meta Signals	Mistranscription
98	20	**From:** There were more, but - - I recall, yeah, more which is **To:** There were more, but - - I recall, yeah, one more which is	Mistranscription
98	21	**From:** identifying bought traffic. **To:** identifying bot traffic.	Mistranscription
98	23	**From:** At a high level, how did Meta identify bought **To:** At a high level, how did Meta identify bot	Mistranscription
99	3	**From:** Why did Meta identify drop bought traffic? **To:** Why did Meta identify and drop bot traffic?	Mistranscription
99	4	**From:** Object to form. **To:** Object to form. Calls for speculation.	Mistranscription
99	12	**From:** What is the primary high table that ranking **To:** What is the primary hive table that ranking	Mistranscription
100	7	**From:** What's the primary high table used by Ads **To:** What's the primary hive table used by Ads	Mistranscription
100	17	**From:** Convergence **To:** Conversions	Mistranscription
102	14	**From:** Meta's Business Tool Events builder **To:** Meta's Business Tool Events Manager	Mistranscription
104	12	**From:** And the current project team was resisting. **To:** And the current project team was resisting it.	Mistranscription
104	22	**From:** I joined, Manish Singhal and myself were the o two **To:** I joined, Manish Singhal and myself were the only two	Typographical

EXHIBIT O

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION
---oOo---

IN RE:
META PIXEL HEALTHCARE LITIGATION
No. 3:22-cv-3580-WHO (VKD)
_____/

HIGHLY CONFIDENTIAL ATTORNEYS' EYES ONLY

30(b)(6) VIDEOTAPED DEPOSITION OF TOBIAS WOOLDRIDGE
PALO ALTO, CALIFORNIA
MONDAY, APRIL 28, 2025

STENOGRAPHICALLY REPORTED BY:
ANDREA M. IGNACIO, CSR, RPR, CRR, CCRR, CLR ~
CSR LICENSE NO. 9830
JOB NO. 7340108

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION
---oOo---

IN RE:
META PIXEL HEALTHCARE LITIGATION
No. 3:22-cv-3580-WHO (VKD)
_____/

30(b)(6) Videotaped Deposition of Tobias Wooldridge, taken on behalf of Plaintiffs, Pursuant to Notice, on Monday, April 28, 2025, at Gibson Dunn & Crutcher, LLP, 310 University Avenue, Palo Alto, California 94301, beginning at 9:18 a.m., and ending at 3:34 p.m., before me, ANDREA M. IGNACIO, CSR, RPR, CCRR, CRR, CLR ~ License No. 9830.

A P P E A R A N C E S:

FOR PLAINTIFFS AND THE PROPOSED CLASS:

SIMMONS HANLY CONROY LLC
By: JASON "JAY" BARNES, Esq.
ERIC JOHNSON, Esq. - Illinois Office
112 Madison Avenue, 7th Floor
New York, New York 10016
212.784.6400
jaybarnes@simmonsfirm.com

- and -

TERRELL MARSHALL LAW GROUP PLLC
By: RYAN TACK-HOOPER, Esq.
936 North 34th Street, Suite 300
Seattle, Washington 98103
206.816.6603
rtack-hooper@terrellmarshall.com

A P P E A R A N C E S: (CONT.)

FOR THE DEFENDANTS:

GIBSON, DUNN & CRUTCHER LLP
By: ELIZABETH KATHARINE MCCLOSKEY, Esq.
ASHLEY ROGERS, Esq. - Dallas Office
NATALIE HAUSKNECHT, Esq. - Denver Office
One Embarcadero Center, Suite 2600
San Francisco, California 94111
415.393.8200
emccloskey@gibsondunn.com

ZOOM ATTENDEES

GIBSON DUNN & CRUTCHER LLP
By: MATT BUONGIORNO, Esq.
MATTHEW REAGAN, Esq. - San Francisco
811 Main Street, Suite 3000
Houston, Texas 77002
214.698.3204
mbuongiorno@gibsondunn.com

A P P E A R A N C E S: (CONT.)

ALSO PRESENT:

Cameron Tuttle, Videographer

Veronica Nauts, Meta in-house counsel

Carrie Bodner, Meta in-house counsel

---oOo---

I N D E X

WITNESS: Tobias Wooldridge - 30(b)(6)

---oOo---

E X H I B I T S

//

//

E X H I B I T S

E X H I B I T S

//

//

E X H I B I T S

E X H I B I T S

---oOo. --

PREVIOUSLY MARKED EXHIBITS

---oOo---

DEPOSITION PROCEEDINGS

MONDAY, APRIL 28, 2025

---oOo---

THE VIDEOGRAPHER: Good morning. We are going on the record. The time is 9:18 a.m. on April 28, 2025.

Please note that the microphones are sensitive and may pick up whispering and private conversations. Please mute your phones at this time.

Audio and video recording will continue to take place, unless all parties agree to go off the record.

This is Media Unit 1 of the video-recorded deposition of Tobias Wooldridge, taken by counsel for Plaintiff.

In the matter of In Re Meta Pixel Healthcare Litigation. Filed in the United States District Court, Northern District of California. Case No. 3:22-cv-3580-WHO.

The location of the deposition is 310 University Avenue, Palo Alto, California 94301.

My name is Cameron Tuttle, representing Veritext. I am the videographer. I am not authorized to administer an oath. I am not related to any party

previously, yes.

Q Okay. What does the term "where the pixel is fired" mean in each of the comment fields excerpted from the schema for offsite_signals?

A For the first four columns listed in this list; City, Country, City ID, and GYP ZIP -- I think there may be a transcription error in GYP ZIP. I thinks that is supposed to be a nondisqual, but...

Q Good point. Thank you.

A For each of those columns, this refers to the location that was estimated based on the IP address that was, you know, sent with the transmission of the pixel data to Meta.

Q So is it the IP address of the Facebook user, a class member in this case, the business using the pixel, or a Meta server?

A For pixel events, this would tend to be the IP address of the device which they're using, unless, for instance, they may be using some sort of relay or proxy or VPN.

Q You say "they." Do you mean the end user, not the website, but the end user is the "they" that you're saying; correct?

MS. MCCLOSKEY: Object to form; vague.

THE WITNESS: When I say -- when I said

"they," I was referring to the person utilizing the device.

MR. BARNES: Okay.

MS. MCCLOSKEY: I'm just going to note for the record that this document was provided to counsel last Thursday at the end of the business day. So in other words, one business day prior to today's deposition. It also did not attach the document that is attached after the first page. So it was a different document than counsel is showing the witness today.

MR. BARNES: Q. Mr. Wooldridge, are you familiar with the offsite_signals table?

A I am familiar with the table.

Q Were you asked to prepare for the Off- -- to testify about the offsite_signals table for this deposition?

MS. MCCLOSKEY: Object to form.

MR. BARNES: We're going to move on. We've wasted enough time with this.

Q So --

MS. MCCLOSKEY: You've wasted enough time with this.

MR. BARNES: Q. -- it's the user; correct? Let's do it by 20 -- I'm -- I'm in the chart on the

Highly Confidential.

STENOGRAPHIC REPORTER: Do you need a rough?

MR. BARNES: Yes. Yes.

(WHEREUPON, the deposition ended at 3:34 p.m.)

---oOo---

CERTIFICATE OF STENOGRAPHIC REPORTER

I, ANDREA M. IGNACIO, hereby certify that the witness in the foregoing remote deposition was by me sworn to tell the truth, the whole truth, and nothing but the truth in the within-entitled cause;

That said remote deposition was taken in shorthand by me, a disinterested person, at the time and place therein stated, and that the testimony of the said witness was thereafter reduced to typewriting, by computer, under my direction and supervision;

That before completion of the deposition, review of the transcript [ ] was [x] was not requested. If requested, any changes made by the deponent (and provided to the reporter) during the period allowed are appended hereto.

I further certify that I am not of counsel or attorney for either or any of the parties to the said deposition, nor in any way interested in the event of this cause, and that I am not related to any of the parties thereto.

Dated: May 7, 2025

_____

ANDREA M. IGNACIO, RPR, CRR, CCRR, CLR, CSR No. 9830

EXHIBIT P

```sql
-- SQL code to select Meta Pixel and geo ZIP codes for users in the state of California

SET NOCOUNT ON;

WITH deduped AS (
    SELECT
        t.h[redacted]   -- the FB ID from meta.ads_pixel_traffic
        t.pixel_id,                          -- ID of the website sending the pixel information
        t.geo_ip_zip,                        -- the ZIP from meta.ads_pixel_traffic
        z.physical_state,                    -- the matched state from usps.zip_details
        CASE
            WHEN t.pixel_id = '1445099202415763' THEN 'TaxAct'
            WHEN t.pixel_id = '288696891835309'  THEN 'H&R Block'
            ELSE 'Unknown'
        END AS company_name,
        ROW_NUMBER() OVER (
            PARTITION BY t.[redacted]
            ORDER BY t.pixel_id
        ) AS rn
    FROM meta.ads_pixel_traffic AS t
    INNER JOIN usps.zip_details AS z
        ON t.geo_ip_zip = z.physical_zip
    WHERE z.physical_state = 'CA'
      AND (t.pixel_id = '1445099202415763' OR t.pixel_id = '288696891835309')
)
SELECT
    [redacted]
    pixel_id,
    geo_ip_zip,
    physical_state
FROM deduped
WHERE rn = 1
ORDER BY
    pixel_id,
    [redacted]
```

EXHIBIT Q

```sql
-- Count the rows that contain tax information

SELECT COUNT(*) AS tax_info_row_count
FROM meta.offsite_signals
WHERE action_source = 'website'
    AND [redacted] = 'used_in_prod'
    AND event_category = 'default'
    AND connection_method IN ('browser','server')
    AND (custom_data_json LIKE '%age_range%'
    OR custom_data_json LIKE '%agi%'
    OR custom_data_json LIKE '%charitable_contribution%'
    OR custom_data_json LIKE '%f1099misc%'
    OR custom_data_json LIKE '%federal_owe_amount%'
    OR custom_data_json LIKE '%federal_refund_amount%'
    OR custom_data_json LIKE '%federal_revenue%'
    OR custom_data_json LIKE '%filing_status%'
    OR custom_data_json LIKE '%investments%'
    OR custom_data_json LIKE '%return_year%'
    OR custom_data_json LIKE '%rpt_revenue%'
    OR custom_data_json LIKE '%schedule_c%'
    OR custom_data_json LIKE '%standard_deduction%'
    OR custom_data_json LIKE '%state_revenue%'
    OR custom_data_json LIKE '%svc_revenue%'
    OR custom_data_json LIKE '%tax_form%'
    OR custom_data_json LIKE '%total_revenue%'
    OR custom_data_json LIKE '%w2%');

SELECT COUNT(*) AS tax_info_not_removed_row_count
FROM meta.offsite_signals
  WHERE action_source = 'website'
    AND [redacted] = 'used_in_prod'
    AND event_category = 'default'
    AND connection_method IN ('browser','server')
    AND ((JSON_VALUE(custom_data_json, '$.age_range') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.age_range'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.age_range') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.agi') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.agi'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.agi') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.charitable_contribution') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.charitable_contribution'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.charitable_contribution') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.f1099misc') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.f1099misc'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.f1099misc') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.federal_owe_amount') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.federal_owe_amount'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.federal_owe_amount') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.federal_refund_amount') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.federal_refund_amount'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.federal_refund_amount') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.federal_revenue') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.federal_revenue'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.federal_revenue') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.filing_status') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.filing_status'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.filing_status') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.investments') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.investments'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.investments') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.return_year') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.return_year'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.return_year') <> '_removed_')
    OR (JSON_VALUE(custom_data_json, '$.rpt_revenue') IS NOT NULL
    AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.rpt_revenue'))) <> ''
    AND JSON_VALUE(custom_data_json, '$.rpt_revenue') <> '_removed_')
```

```
OR (JSON_VALUE(custom_data_json, '$.schedule_c') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.schedule_c'))) <> ''
AND JSON_VALUE(custom_data_json, '$.schedule_c') <> '_removed_')
OR (JSON_VALUE(custom_data_json, '$.standard_deduction') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.standard_deduction'))) <> ''
AND JSON_VALUE(custom_data_json, '$.standard_deduction') <> '_removed_')
OR (JSON_VALUE(custom_data_json, '$.state_revenue') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.state_revenue'))) <> ''
AND JSON_VALUE(custom_data_json, '$.state_revenue') <> '_removed_')
OR (JSON_VALUE(custom_data_json, '$.svc_revenue') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.svc_revenue'))) <> ''
AND JSON_VALUE(custom_data_json, '$.svc_revenue') <> '_removed_')
OR (JSON_VALUE(custom_data_json, '$.tax_form') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.tax_form'))) <> ''
AND JSON_VALUE(custom_data_json, '$.tax_form') <> '_removed_')
OR (JSON_VALUE(custom_data_json, '$.total_revenue') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.total_revenue'))) <> ''
AND JSON_VALUE(custom_data_json, '$.total_revenue') <> '_removed_')
OR (JSON_VALUE(custom_data_json, '$.w2') IS NOT NULL
AND LTRIM(RTRIM(JSON_VALUE(custom_data_json, '$.w2'))) <> ''
AND JSON_VALUE(custom_data_json, '$.w2') <> '_removed_'));
```